高等职业教育“十二五”规划教材

计算机网络安全技术

耿　杰◎主　编
王　俊　白悍东　彭庆红　张　卫◎副主编

- 提供PPT课件
- 配备习题答案
- 知识讲解+上机实训
- 轻理论、重应用，符合高职教学特点

配套资源下载地址：http://www.tup.com.cn

清华大学出版社

高等职业教育“十二五”规划教材

计算机网络安全技术

耿　杰　主　编

王　俊　白悍东　彭庆红　张　卫　副主编

清华大学出版社

北　京

内 容 简 介

目前，计算机网络安全已经引起了社会的普遍关注，成为当今网络技术的一个重要研究课题。本书以计算机网络安全技术为主要内容，着重讲述了计算机网络安全的基本理论和基本安全技术。主要内容包括计算机网络安全概述、密码技术、网络通信协议与安全、Windows Server 2003 网络安全与策略、防火墙应用技术、入侵检测技术、网络病毒安全、黑客的攻击与防范、Web 安全与维护等。

本教材以职业能力培养为主线，安排了大量的实训内容，既适合高职高专计算机网络专业及相关专业学生使用，也可作为计算机网络安全类的技术参考书和培训教材。

图书在版编目（CIP）数据

计算机网络安全技术/耿杰主编．—北京：清华大学出版社，2013
高等职业教育“十二五”规划教材

ISBN 978-7-302-33311-1

I. ①计…　II. ①耿…　III. ①计算机网络-安全技术-高等职业教育-教材　IV. ①TP393.08

中国版本图书馆 CIP 数据核字（2013）第 173627 号

责任编辑：苏明芳
封面设计：刘　超
版式设计：文森时代
责任校对：李虎斌
责任印制：
出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：
装 订 者：
经　　销：全国新华书店
开　　本：185mm×260mm　**印　　张：**13.25　**字　　数：**295 千字
版　　次：2013 年 10 月第 1 版　**印　　次：**2013 年 10 月第 1 次印刷
印　　数：1～2400
定　　价：29.00 元

产品编号：040749-01

前　　言

随着信息技术的迅猛发展和广泛应用，社会信息化进程不断加快，信息网络的基础性、全局性作用日益增强，社会对计算机网络的依赖性越来越大。随之而来的是计算机网络安全问题。普及计算机网络安全知识以及从法律上、技术上确保计算机网络的安全，已成为保护我国计算机网络安全的头等大事。鉴于此，为高职高专计算机及其相关专业的学生开设计算机网络安全技术课是十分必要的。

在编写本教材时，密切结合高职职业性、实践性、适应性、针对性的特点，对于计算机网络安全技术的理论知识和工作原理介绍的简单一些，而更多的内容侧重于对计算机具体网络安全技术应用的介绍。全书共分 9 章，通俗地阐述了网络所涉及的安全问题及各种相关的安全技术及应用。主要内容包括计算机网络安全概述、密码技术、网络通信协议与安全、Windows Server 2003 网络安全与策略、防火墙应用技术、入侵检测技术、网络病毒安全、黑客的攻击与防范以及 Web 安全与维护。

第 1 章是计算机网络安全概述，主要内容包括计算机网络安全简介、网络安全面临的威胁及原因、网络安全机制；第 2 章是密码技术，介绍了数据加密标准 DES 等常见的加密算法，同时详细介绍了加密技术的典型应用——数字签名的实现方法；第 3 章是网络通信协议与安全，介绍了网络通信的安全性、网络通信存在的安全威胁等；第 4 章是 Windows Server 2003 网络安全与策略，主要以 Windows Server 2003 为基础，讲述了操作系统的安全机制、安全管理及安全应用；第 5 章是防火墙应用技术，内容包括防火墙的简介、类型、配置，防火墙的选购和使用，常见的防火墙产品介绍；第 6 章是入侵检测技术，内容包括入侵检测简介、类型、配置、选购和使用，以及常见的入侵检测系统；第 7 章是网络病毒安全，介绍了计算机网络病毒的检测、防范和清除的常用技术；第 8 章是黑客的攻击与防范，主要介绍了常用的黑客攻击方法及常用的防黑措施；第 9 章是 Web 安全与维护，主要内容包括 Web 技术简介、Web 服务器安全、Web 浏览器安全等。

本书内容安排合理，逻辑性强，文字简明，循序渐进，通俗易懂。书中提供了大量的网络安全技术实训，读者通过实训项目的操练，可以掌握计算机网络安全的基本原理与技术，进而增强对实际问题的处理能力。为方便教学，本书配有电子课件以及习题答案，读者可到清华大学出版社网站下载。该书适合高职高专计算机网络技术及其相关专业学生使用，也可作为计算机网络安全的培训教材，对从事信息安全的人员也是一本技术应用参考书。

本书在编写过程中得到了许多专家和同仁以及清华大学出版社编辑的大力支持，在此向他们表示最真挚的感谢！

由于作者水平有限，书中不免有疏漏和不足之处，欢迎广大读者批评指正。主编邮箱：ruopiao97121@163.com（耿杰）。

编　者

目　　录

第 1 章 计算机网络安全概述

知识目标

- 掌握网络安全的定义。
- 掌握网络面临的各种安全威胁。
- 了解产生网络安全威胁的原因。
- 了解计算机系统的安全等级。

技能目标

- 能识别网络威胁的类别。
- 熟练使用网络工具对计算机系统进行漏洞扫描。
- 能区分常用计算机系统的安全级别。

随着 Internet 的不断发展，网络上丰富的信息资源给用户带来了极大的方便，但同时也给上网用户带来了安全问题。由于 Internet 的开放性、超越组织与国界等特点，使它在安全性上存在一些隐患，而且信息安全的内涵也发生了一些变化。目前，网络安全问题已经在许多国家引起了普遍关注，成为当今网络技术的一个重要研究课题。

1.1 计算机网络安全简介

目前，Internet 几乎覆盖了世界各地，容纳了数十万个网络，为几十亿用户提供了形式多样的网络与信息服务。除了广泛应用的 Web 网页、E-mail、新闻论坛等文本信息的交流与传播外，网络电话、网络传真、视频等通信技术都在迅猛地发展。在信息化社会中，计算机网络将在政治、军事、金融、商业、交通、电信、文教等方面发挥越来越重要的作用。社会对网络的依赖日益增强。人们依靠计算机网络系统接收和处理信息，实现相互间的联系和对目标的管理、控制。通过网络交流信息、获得信息已成为现代信息社会的一个主要特征。网络正改变着人们的工作方式和生活方式。

科技进步在造福人类的同时，也带来了新的危害。随着网络的开放性、共享性和互联程度的扩大，特别是 Internet 的出现，网络的重要性和对社会的影响越来越大，随之相伴的是由于网络的脆弱性，利用计算机网络犯罪的情况越来越严重，已经严重地危害了社会的发展和国家的安全。

1989 年 10 月，WANK（Worms Against Nuclear Killers）蠕虫入侵 NASA（美国宇航局）可能是历史上第一次有记载的系统入侵。某个家伙为了抗议“钚”驱动的伽利略探测器的发射而入侵了 NASA 系统，造成了约 50 万美金的损失。

1996 年 8 月 14 日，美国发生一起计算机病毒入侵计算机网络的事件，几千台计算机被病毒感染，Internet 不能被正常访问。政府不得不立即做出反应，国防部成立了计算机快速行动小组。这次病毒事件导致的直接经济损失达 1 亿多美元。

2000 年 1 月，昵称 Maxim 的黑客侵入 CD Universe 购物网站并窃取了 30 万份信用卡资料。

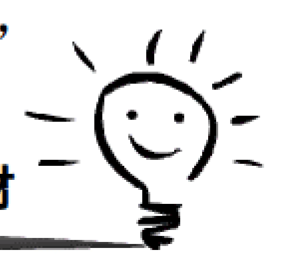
2003 年 3 月 21 日，黑客侵入了江苏某信息网的多台服务器，破译了密码数据库，获得了网络工作人员的口令和 300 多个合法用户的账户与密码，并将这些密码和口令公布于众。

2008 年 2 月，一黑客利用无线刷卡设备的漏洞入侵了美国两家大型连锁超市 Hannaford 和 Sweetbay，盗窃了 1800 份完整的信用卡资料和 420 万份信用卡的部分资料。

2011 年，国内新增木马等恶意程序数量高达 4.48 亿个，平均每秒出现 29 个新木马，相比 2010 同期暴涨 346%。游戏外挂、在线视频、伪装图片以及破解软件是木马病毒的四大“重灾区”，平均每天约 453 万台计算机受到木马的攻击。

事实上，上面这些网络入侵事件只是我们知道的实际所发生的事例中非常微小的一部分，有相当多的网络入侵或攻击并没有被发现，或者出于各种各样的原因未被公开。

面对越来越严重的计算机网络安全的威胁，必须采取措施来保证计算机网络的安全。但是现有的计算机网络大多数在设计的开始都忽略了安全问题，即使有的考虑了安全问题，



大部分都是把安全机制建立在物理安全上。随着网络的互联程度的扩大，这种安全机制对于网络环境来讲很脆弱。同时，目前网络上使用的协议，如 TCP/IP 协议，在制定之初也没有把安全考虑在内，所以网络协议本身就是不设防的，其存在很多的安全问题，不能满足网络安全要求。另外，网络的开放性和资源共享也是安全问题的一个主要根源，解决这个问题主要依赖于加密、网络用户身份鉴别、存取控制策略等技术手段。

一个安全的网络体系至少应包括 3 类措施：法律措施、技术措施、政策措施。面对计算机网络安全的种种威胁，仅仅利用物理上和政策上的手段是十分有限和困难的，因此也应采用逻辑上的措施，即研究开发有效的网络安全技术，例如安全协议、密码技术、数字签名、防火墙、安全管理、安全审计等，以防止网络上传输的信息被非法窃取、篡改、伪造，保证其保密性和完整性；防止非法用户的侵入，限制网络上用户的访问权限，保证信息存放的私有性。除了私有性和完整性外，一个安全的计算机网络还必须考虑通信双方身份的真实性和信息的可用性。

计算机网络安全的目的是要保证网络上数据存储和传输的安全性。国内外很多研究机构为了解决这个问题做了大量的工作，主要有数据加密、身份认证、数字签名、防火墙、安全审计、安全管理、安全内核、安全协议、IC 卡、拒绝服务、网络安全性分析、网络信息安全监测和信息安全标准化等方面的研究。

1.1.1　计算机网络安全的概念

1. 什么是计算机网络安全

计算机网络安全是指保持网络中的硬件系统和软件系统正常运行，使它们不因自然和人为的因素而受到破坏、更改和泄露。网络安全主要包括物理安全、软件安全、信息安全和运行安全 4 个方面。

（1）物理安全。

物理安全包括硬件、存储介质和外部环境的安全。硬件是指网络中的各种设备和通信线路，如主机、路由器、服务器、工作站、交换机、电缆等；存储媒介质包括磁盘、光盘等；外部环境则主要指计算机设备的安装场地、供电系统。保障物理安全，就是要保护这些硬件设施能够正常工作而不被损害。

（2）软件安全。

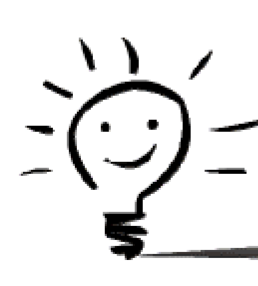
软件安全是指网络软件以及各个主机、服务器、工作站等设备所运行的软件的安全。保障软件安全，就是保护网络中的各种软件能够正常运行而不被修改、破坏和非法使用。

（3）信息安全。

信息安全是指网络中所存储和传输数据的安全，主要体现在信息隐蔽性和防修改的能力上。保障信息安全，就是保护网络中的信息不被非法修改、复制、解密、使用等，也是保障网络安全最根本的目的。

（4）运行安全。

运行安全指网络中的各个信息系统能够正常运行并能正常地通过网络交流信息。保障运行安全，就是通过对网络系统中的各种设备运行状况进行监测，发现不安全因素时，及



时报警并采取相应措施，消除不安全状态以保障网络系统的正常运行。

网络安全的目的是为了确保网络系统的保密性、完整性和可用性。保密性要求只有授权用户才能访问网络信息；完整性要求网络中的数据保持不被意外或恶意地修改；可用性指网络在不降低使用性能的情况下仍能根据授权用户的需要提供资源服务。

1.1.2　网络安全的特征

由于网络安全受到威胁的多样性、复杂性及网络信息、数据的重要性，在设计网络系统的安全时，应该努力达到安全目标。一个安全的网络具有下面 5 个特征：可靠性、可用性、保密性、完整性和不可抵赖性。

（1）可靠性。

可靠性是网络安全最基本的要求之一，是指系统在规定条件下和规定时间内完成规定功能的概率。如果网络不可靠、经常出问题，这个网络就是不安全的。目前，对于网络可靠性的研究主要偏重于硬件可靠性方面。研制高可靠性硬件设备，采取合理的冗余备份措施是最基本的可靠性对策。但实际上有许多故障和事故，与软件可靠性、人员可靠性和环境可靠性有关。人员可靠性在通信网络可靠性中起着重要作用，有关资料表明，系统失效中很大一部分是由人为因素造成的。

（2）可用性。

可用性是可被授权实体访问并按需求使用的特性，即当需要时能否存取所需的信息。网络最基本的功能是向用户提供所需的信息和通信服务，而用户的通信要求是随机的、多方面的，有时还要求时效性。网络必须随时满足用户通信的要求。从某种意义上讲，可用性是可靠性的更高要求，特别是在重要场合下，特殊用户的可用性显得十分重要。为此，网络需要采用科学合理的网络拓扑结构、必要的冗余、容错和备份措施以及网络自愈技术、分配配置和负荷分担、各种完善的物理安全和应急措施等，从满足用户的需求出发，保证通信网络的安全。网络环境下拒绝服务、破坏网络和有关系统的正常运行等都属于对可用性的攻击。

（3）保密性。

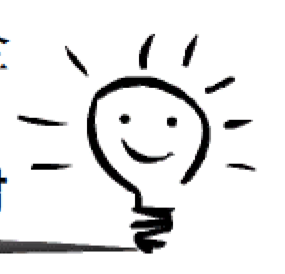
保密性指信息不被泄漏给非授权用户、实体或过程，信息只被授权用户使用。保密性是对信息的安全要求，它是在可靠性和可用性的基础上，保障网络中信息安全的重要手段。对于敏感用户信息的保密，是人们研究最多的领域。由于网络信息会成为黑客、计算机犯罪、病毒、甚至信息战的攻击目标，已受到了人们越来越多的关注。

（4）完整性。

完整性也是面向信息的安全要求。它是指信息不会被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等操作破坏的特性。它与保密性不同，保密性是防止信息泄漏给非授权的用户，而完整性则要求信息的内容和顺序都不受破坏和修改。用户信息和网络信息都要求完整性，例如涉及金融的用户信息，如果用户账目被修改、伪造或删除，将带来巨大的经济损失。网络中的网络信息一旦受到破坏，严重的还会造成通信网络的瘫痪。

（5）不可抵赖性。

不可抵赖性也称作不可否认性，是面向通信双方（人、实体或进程）信息真实的安全



要求。它包括收发双方均不可抵赖。随着通信业务的不断扩大，电子贸易、电子金融、电子商务和办公自动化等许多信息处理过程都需要通信双方对信息内容的真实性进行认同，为此，应采用数字签名、认证、数据完备、鉴别等有效措施，以实现信息的不可抵赖性。

网络的安全不仅仅是防范窃密活动，其可靠性、可用性、完整性和不可抵赖性应作为与保密性同等重要的安全目标加以实现。我们应从观念上、政策上做出必要的调整，全面规划和实施网络信息的安全。

1.2　计算机网络面临的威胁

1.2.1　网络内部威胁

1. 计算机系统的脆弱性

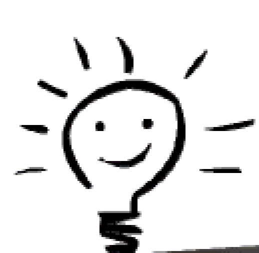
计算机系统的脆弱性主要来自计算机操作系统的不安全性，在网络环境下，还来源于网络通信协议的不安全性。计算机系统有其自身的安全级别，有关安全等级的定义我们将在 1.4.2 节详细讨论。有的计算机操作系统属于 D 级，这一级别的操作系统根本就没有安全防护措施，它就像一个门窗大开的房间，如 DOS、Windows 3.x、Windows 95 等操作系统，它们只能用于一般的桌面计算机系统，而不能用于安全性要求高的服务器的操作系统。UNIX 系统和 Windows XP/2000/2003 达到了 C2 级别，其安全性远远强于 Windows 95 操作系统，而且主要用于服务器上。但这类操作系统仍然存在着安全漏洞，因为它们中都存在超级用户，UNIX 中是 root，而 Windows XP/2000/2003 中是 Administrator，如果入侵者得到了超级用户口令，整个系统将完全受控于入侵者，这样系统就面临着巨大的危险。现在，人们正在研究一种新型的操作系统，在这种操作系统中没有超级用户，也就不会存在超级用户带来的问题。现在很多操作系统都使用静态口令，但口令还是有很大的被破解的可能性，而且不好的口令维护制度会导致口令丢失。口令丢失也就意味着安全系统的全面崩溃。

世界上没有能长久运行的计算机系统，计算机系统可能会因硬件故障或软件原因而停止运行或运行错误，或被入侵者利用并造成损失。硬盘故障、电源故障和主板芯片故障等都是人们应经常考虑的硬件故障问题。软件原因可能存在于操作系统中，更多的是存在于应用软件中。

2. 来自网络内部的威胁

对网络内部的威胁主要是来自网络内部的用户，这些用户试图访问那些不允许使用的资源和服务器。可以分为两种情况，一种是有意的安全破坏，入侵者的攻击和计算机犯罪就属于这一类。这是计算机网络所面临的最大威胁，此类攻击还可以分为主动攻击和被动攻击两种情况，主动攻击是指计算机网络的内部用户以各种方式有选择地破坏信息的有效性和完整性；而被动攻击则是在不影响网络正常工作的情况下，进行信息截获、窃取、破译等，目的是为了获得重要机密信息。

第二种内部威胁是由于用户安全意识差造成的无意识的操作失误，使得系统或网络误



操作或崩溃。如操作员安全配置不当造成的安全漏洞或隐患、用户安全意识不强、用户口令选择不慎或不恰当、用户将自己的账号保护不严或与别人共享等都会对网络安全带来威胁和隐患，或者被非法入侵者加以利用，从而造成对系统的危害。

1.2.2 网络外部威胁

除了受到来自网络内部的安全威胁外，网络还受到来自外界的各种各样的威胁。网络系统受到的威胁是多样的，因为在网络系统中可能存在许多种类的计算机和操作系统，采用统一的安全措施是不容易的，也是不可能的，而对网络进行集中安全管理则是一种好的方案。

网络受到的外部威胁可以归结为物理威胁、网络威胁、身份鉴别、病毒、黑客、系统漏洞等。

1. 物理威胁

物理安全是指保护计算机硬件和存储介质等设备和工作程序不遭受损失。

网络的物理安全是整个网络系统安全的前提，总体来说物理威胁主要有：地震、水灾、火灾等环境事故；电源故障；人为操作失误或错误；设备被盗、被毁；电磁干扰；线路截获；高可用性的硬件；双机多冗余的设计；机房环境及报警系统、安全意识等。网络工程建设中，由于网络系统属于弱电工程，耐压值很低。因此，在网络工程的设计和施工中，必须优先考虑保护人和网络设备不受电、火灾和雷击的侵害；考虑布线系统与照明电线、动力电线、通信线路、暖气管道及冷热空气管道之间的距离；考虑布线系统和绝缘线、裸体线以及接地与焊接的安全；必须建设防雷系统，防雷系统不仅考虑建筑物防雷，还必须考虑计算机及其他弱电耐压设备的防雷。

2. 网络威胁

计算机网络的发展和使用对数据信息造成了新的安全威胁。在计算机网络上存在着电子窃听，因为分布式计算机系统的特征是各种分离的计算机通过一些媒介相互连接在一起，进行相互通信，而且局域网一般是广播式的，因此只要把网卡模式设置成混合模式，网络上人人都可以收到发向任何人的信息。当然，也可以通过加密来解决这个问题，但目前，强大的加密技术还没有在网络上广泛使用，况且加密也是有可能被破解的。

网络设备的因素可以构成网络的安全威胁。我国的很多个人网络用户都是通过调制解调器+电话线方式拨号接入 Internet 或自己单位的局域网的，因为调制解调器也存在安全问题，入侵者就可能通过电话线入侵到用户的网络中去。

在 Internet 上还存在着很多电子欺骗的现象，而这种电子欺骗的形式也是多种多样的。如一个公司可能会谎称一个站点是他们公司的网站，或者在网络通信中，有的人可能冒充别人或冒充从另外一台机器访问某站点等，这样会很难辨别用户的真实身份。

3. 身份鉴别

生活中时常要用到身份鉴别，这里说的身份鉴别是指计算机判断用户是否使用它的一



种过程。目前，身份鉴别普遍存在于计算机系统当中，实现的方式各种各样，有的功能十分强大，有的则比较脆弱。其中，口令就是一种比较脆弱的身份鉴别手段，它的功能不是很强，但因为实现起来比较简单，所以还是被广泛采用。计算机系统的身份鉴别中存在口令圈套、口令破解和算法缺陷等安全威胁。

口令圈套是一种十分高明的诡计，它是靠欺骗来获取口令的手段。如登录欺骗，即人为写出一个代码模块，运行起来像登录屏幕一样，并把它插入到登录过程之前，这样，用户就会把用户名和登录口令告知程序，这个程序会把用户名和口令保存起来。除此之外，该代码还会告诉用户登录失败，并启动真正的登录程序，这样用户就不容易发现这个欺骗。

还有一种得到口令的方式是用密码字典或其他工具软件来暴力破解口令，有的用户选用的口令十分脆弱，如一个人的生日、电话号码、名字或单词等，这样攻击者利用计算机的速度就很容易强行破解。因此系统管理员应对用户的口令进行严格审查，通常可以利用一些工具软件来检查口令是否达到系统管理的要求和规定。

4. 病毒

目前计算机数据安全的头号大敌是计算机病毒，它是编制者在计算机程序中插入的破坏计算机功能或数据，影响计算机软件、硬件的正常运行并且能够自我复制的一组计算机指令或程序代码。计算机病毒具有传染性、寄生性、隐蔽性、触发性、破坏性等特点。因此，提高对病毒的防范刻不容缓。

5. 黑客

对于计算机数据安全构成威胁的另一个方面是来自电脑黑客（hacker）。电脑黑客利用系统中的安全漏洞非法进入他人计算机系统，其危害性非常大。从某种意义上讲，黑客对信息安全的危害甚至比一般的计算机病毒更为严重。

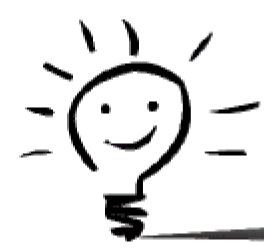
6. 系统漏洞

系统漏洞是指应用软件或操作系统软件在逻辑设计上的缺陷或在编写时产生的错误，这些缺陷或错误恰恰是黑客进行攻击的首选目标，通过这些缺陷或错误植入木马、病毒等方式来攻击或控制整个计算机，从而窃取计算机中的重要资料和信息，甚至破坏计算机系统。

漏洞影响到的范围很大，包括系统本身及其支撑软件、网络客户和服务器软件、网络路由器和安全防火墙等。换言之，在这些不同的软、硬件设备中都可能存在不同的安全漏洞问题。

1.2.3　网络安全防范措施

操作系统的价值是由系统性能、安全管理花费的时间、使用性和复杂性决定的。很多操作系统设有系统“安全员”专门管理和监控计算机系统设备的安全运转。安全措施有很多形式，可以是将操作系统设置成阻止用户读取未经批准的数据，不允许用户越权读取数



据信息。它可以是计算机用户的工作步骤，比如在碎纸机或者焚烧炉中处理所有的打印资料或磁介质；也可以是以报警和日志的形式，告诉管理员在什么时候有人试图闯入或闯入成功。安全措施还包括在操作人员接触秘密数据前，对他们进行广泛的安全检查。安全措施也可以是保障物理安全的形式，比如门上锁和设报警系统以防止偷窃设备和存储介质等。

在安全环境中，许多安全措施相互加强，如果一层失败，则另一层将防止或最大限度地减少损害。下面是一些具体的措施。

1. 数据信息的备份

备份或复制重要的数据，并将复制或备份保留在一个安全的地方，一旦失去原件就能使用备份。应该有规律地备份以避免由于硬件故障导致的数据信息的丢失。提高可靠性是提高安全性的一种方法，备份就是一种提高系统可靠性的方法，它可以保证今天存储的数据明天还可以使用。由于计算机系统芯片或者电源的失效，甚至是火灾等可能引起系统的失误或破坏，备份将提高安全保障。

备份对于防范人为的破坏也至关重要。如果计算机系统被破坏，只要有数据备份，就可以在另一台计算机上恢复。备份系统是最常用的提高数据完整性的措施，备份工作可以手工完成，也可以自动完成，现有的操作系统，如 NetWare、Windows 2000 和 UNIX 等都自带有备份系统，但这种备份系统比较初级，如果对备份要求高，就要配置专用的备份系统。

2. 病毒检查

定期检查病毒并对移动存储介质、下载的文件或软件加以安全控制，最起码应在使用前对移动存储介质和下载的软件进行病毒检查，及时更新杀毒软件的版本，注意病毒流行的动向，及时发现正在流行的计算机病毒，并采取相应的措施进行防范。

3. 及时安装补丁程序

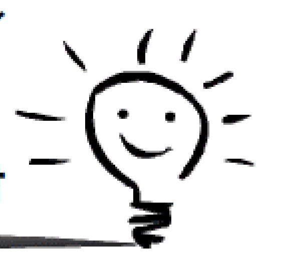
计算机操作系统和应用系统软件都会存在一些漏洞，这些漏洞可以通过软件商提供的补丁程序进行修正，因此及时安装各种安全补丁程序，不要给入侵者可乘之机。系统的安全漏洞传播很快，若不及时修正，后果就难以预料。现在，一些大公司的网站上都有这种系统安全漏洞的说明，并有相应的解决方法，用户可以访问这些站点以获取有用的信息，或对软件进行自动更新，如 Windows XP、Windows 2000、Windows Server 2003 等系统就可以进行自动更新。

4. 提高物理安全

保证机房的物理安全，因为即使采取了网络安全或其他安全措施，如果有人闯入机房，那么所有措施都不是很管用了。因此，保证计算机机房的安全是提高物理安全的重要保证。

5. 设置 Internet 防火墙

Internet 防火墙是一种有效保证网络安全的技术，但一个维护很差的防火墙对网络安全也不会有很大的作用，所以还需要一个有经验的防火墙管理和维护人员。虽然防火墙是网络安全体系中极为重要的一环，但它并不是万能的，不能因为有防火墙就认为可以高枕无忧。虽然防火墙可以解决一些安全问题，防火墙的应用应该受到充分的重视，但仍有很多



危险是防火墙解决不了的，防火墙并不能解决所有的安全问题。

防火墙不能防止内部的攻击，因为它只提供了网络边界的防卫，内部的人员可以滥用访问权限，从而引起安全事故。事实上，许多黑客入侵事件和 Internet 的关系很小，如一种常用的入侵手段是社会工程攻击，它就是靠欺骗获得一些可以破坏安全的信息，如网络口令等。另外，一些用来传递数据的电话线也很有可能被用来作为入侵内部网络的途径。

恶意的代码也是防火墙不能解决的一个问题，如病毒和特洛伊木马，而 E-mail 和 Java 的使用则为病毒的传播带来了方便。虽然现在的防火墙可以检查病毒和特洛伊木马，但这些防火墙只能阻挡已知的病毒程序，这就可能让新的病毒或特洛伊木马侵入系统。而且，特洛伊木马不仅来自网络，也可能来自软盘、光盘和移动存储设备，因此，要有相应的制度，对网络和磁盘进行严格检查。

如果没有明确的信息安全制度，即使拥有再好的防火墙也没有用。在建立局域网时如果没有做好 PC 机的安全措施，当把局域网连入 Internet 时，就不能保证局域网的安全了。

6. 审查日志

阅读审查日志文件，我们可以发现被入侵的痕迹，以便及时采取弥补措施，或追踪入侵者。对可疑活动一定要进行仔细分析，例如，有人在试图访问一些不安全的服务端口，利用扫描工具、木马程序等手段访问用户的服务器，最典型的情况就是有人多次企图登录到用户的机器上，但会遭到多次失败，特别是试图登录到 Internet 上的通用账户。

7. 数据加密

现代加密技术很发达。为防止网络被窃听和劫持，可以对网络通信加密，对绝密文件更应该实施加密，以保证数据或数据通信的可靠和安全。

1.3　网络安全体系结构

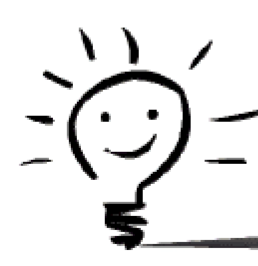
网络安全体系的安全目标是系统的保密性、完整性与可用性的具体化。1989 年，为实现开放系统互联网环境下的信息安全，ISO/TC97 技术委员会制定了 ISO7498-2 国际标准。该标准从体系结构的观点，描述了实现 OSI 参考模型之间的安全通信所必需提供的安全服务和安全机制，建立了开放系统互联标准的安全体系结构框架，为网络安全的研究奠定了基础。

1.3.1　安全服务

ISO7498-2 提供了以下 5 种可供选择的安全服务。

1. 鉴别

鉴别是访问控制的基础，是针对主动攻击的重要防御措施。鉴别服务包括两类：一是对等实体鉴别服务，这种服务是在两个开放系统（OSI）同等层中的实体建立连接和数据传送期间，为提供连接实体身份的鉴别而规定的一种服务，这种服务防止假冒或重放以前的连接，也防止伪造连接初始化这种类型的攻击。这种鉴别服务可以是单向的，也可以是双



向的。另一类是数据源鉴别服务，就是某一层向上一层提供的服务，它用来确保数据是由对等实体发出的，对上一层提供数据源的对等实体进行鉴别，以防假冒。

2. 访问控制

访问控制的目的是控制不同用户对信息资源的访问权限，是针对越权使用资源的防御措施。访问控制可分为自主访问控制和强制访问控制两类。实现机制可以是基于访问控制属性的访问控制表（或访问控制矩阵），也可以是基于安全标签、用户分类及资源分档的多级控制。

3. 数据保密

这种服务的目的是保护网络中各系统之间交换的数据，防止因数据被截获而造成的泄密。可分为以下几种。

（1）连接保密：对某个连接上的所有用户数据提供保密。

（2）无连接保密：对一个无连接的数据包的所有用户数据提供保密。

（3）选择字段保密：对一个协议数据单元中的用户数据的一些经选择的字段提供保密。

4. 数据完整性

数据完整性是针对非法篡改信息而设置的防范措施。指的是防止网上所传输的数据被修改、删除、插入、替换或重发，从而保护合法用户接收和使用该数据的真实性。

5. 防止否认

接收方要求发送方保证不能否认接收方收到的信息是发送方发出的信息，而非他人冒名、篡改过的信息；发送方也要求接收方不能否认已经收到的信息。防止否认是针对对方进行否认的防范措施，用来证实已经发生过的操作。

1.3.2 安全机制

为了实现上面各种安全服务，安全体系结构提出了下面 8 种安全机制。

1. 加密机制

加密是提供数据保密的最常用方法。用加密的方法与其他技术相结合，可以提供数据的保密性和完整性。除了对话层不提供加密保护外，加密可在其他各层上进行。与加密机制伴随而来的是密钥管理机制。

2. 访问控制机制

访问控制根据实体的身份及其有关信息，来决定该实体的访问权限。它可以防止未经授权的用户非法使用系统资源，这种服务不仅可以提供给单个用户，也可以提供给用户组的所有用户。访问控制是一种通过对访问者的有关信息进行检查来限制或禁止访问者使用资源的技术，分为高层访问控制和低层访问控制。高层访问控制包括身份检查和权限确认，是通过对用户口令、用户权限、资源属性的检查和对比来实现的。低层访问控制是通过对通信协议中的某些特征信息的识别和判断，来禁止或允许用户访问的措施，如在路由器上

设置过滤规则进行包过滤就属于低层访问控制。

3. 数据完整性机制

数据完整性机制包括两个方面，即数据单元的完整性和数据序列的完整性。

数据单元的完整性是指组成一个单元的一段数据不被破坏和增删篡改。通常是把包括有数字签名的文件用 HASH 函数产生一个标记，接收者在收到文件后也用相同的 HASH 函数处理一遍，看看产生的标记是否相同就可知道数据是否完整。

数据序列的完整性是指将发出的数据分割为按序列号编排的许多单元，在接收时还能按原来的序列把数据串联起来，而不会发生数据单元的丢失、重复、乱序、假冒等情况。

4. 数字签名机制

数字签名机制是以交换信息的方式来确认对象身份的方法，主要解决以下安全问题。

（1）否认：发送者事后不承认自己发送过接收者提供的文件。

（2）伪造：有人伪造了一份文件，却声称是某人发送的。

（3）冒充：冒充别人的身份在网上发送文件。

（4）篡改：接收者对收到的信息进行部分篡改，破坏原意。

数字签名机制具有可证实性、不可否认性、不可伪造性和不可重用性。

5. 交换鉴别机制

交换鉴别机制通过互相交换信息的方式来确定彼此的身份。常用的交换鉴别的技术有以下几种。

（1）口令：由发送方给出自己的口令，以证明自己的身份，接收方则根据口令来判断对方的身份。

（2）密码技术：发送方和接收方各自掌握的密钥是成对的。接收方在收到已加密的信息时，通过自己掌握的密钥解密，能够确定信息的发送者是掌握了另一个密钥的那个人。在许多情况下，密码技术还和时间标记、同步时钟、双方或多方握手协议、数字签名、第三方公证等相结合，以提供更加完善的身份鉴别。

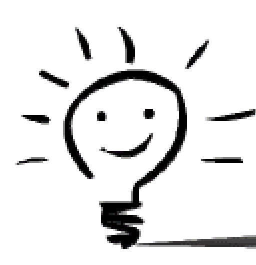
（3）特征实物：例如 IC 卡、指纹、声音频谱等。

6. 公证机制

在一个大型网络中，使用这个网络的所有用户并不都是诚实可信的，同时也可能由于系统故障等原因使传输中的信息丢失、迟到等，这很可能引起谁承担责任的问题。解决这个问题，就需要有一个各方都信任的实体——公证机构，来提供公证服务，仲裁出现的问题。一旦引入公证机制，通信双方进行数据通信时必须经过这个机构来转换，以确保公证机构能得到必要的信息，供以后仲裁。

7. 业务流量填充机制

这种机制主要是对抗非法者在线路上监听数据并对其进行流量和流向分析。攻击者有时能够根据数据交换的出现、消失、数量或频率而提取有用信息。数据交换量的突然改变也可能泄露有用信息。例如当公司开始出售它在股票市场上的份额时，在消息公开以前的



准备阶段中，公司可能与银行有大量通信。因此对购买该股票感兴趣的人就可以密切关注公司与银行之间的数据流量以了解是否可以购买。

流量填充机制能够保持流量基本恒定，因此观测者不能获取任何信息。流量填充的实现方法是随机生成数据并对其加密，再通过网络发送。

8. 路由控制机制

路由控制机制可根据信息发送者的申请选择安全路径。这样，可以选择那些可信的网络节点，从而确保数据不会暴露在安全攻击之下。而且，如果数据进入某个没有正确安全标志的专用网络时，网络管理员可以选择拒绝该数据包。

1.4 计算机系统的安全评估

计算机系统的安全评估是对系统安全性的检验和监督。系统安全评估包括了构成计算机系统的物理网络和系统的运行过程、系统提供的服务以及这种过程与服务中的管理、保证能力的安全评估。一般来说包括：

- ☑ 明确该系统的薄弱环节。
- ☑ 分析利用这些薄弱环节进行威胁的可能性。
- ☑ 评估如果每种威胁都成功所带来的后果。
- ☑ 估计每种攻击的代价。
- ☑ 估算出可能的应对措施的费用。
- ☑ 选取恰当的安全机制。

计算机系统的安全评估可以确保系统连续正常运行，确保信息的完整性和可靠性，及时发现系统存在的薄弱环节，采取必要的措施，杜绝不安全因素。另外，有了安全评估，并不意味着可以高枕无忧，因为要在技术上做到完全的安全保护是不可能的。所以，评估的目标应该是：使攻击所花的代价足够高，从而把风险降低到可接受的程度。

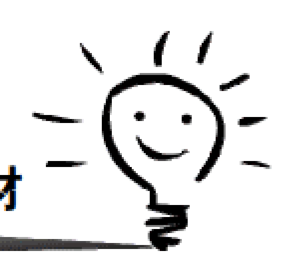
由于计算机系统用途及应用范围的不断扩大，不同的环境对系统可靠性、安全性、保密性的要求各不相同，这就要求有一个定量或定性的安全评估标准。这样的标准是系统安全评估的依据，也是计算机软硬件生产厂家衡量其产品是否符合系统安全要求的依据。它不仅有利于产品安全的规范化，同时也有利于保证产品安全的可信性、可更新和可扩展性。这个安全评估标准的重要性在于以下几个方面。

（1）用户可依据标准，选用符合自己应用安全级别的、评定了安全等级的计算机系统，然后，在此基础上采取安全措施。

（2）一个计算机系统是建立在相应的操作系统之上的，离开了操作系统的安全，也就无法保证整个计算机系统的安全。所以，软件生产厂商应该满足用户的需求，提供各种安全等级的操作系统。

（3）建立系统中其他部件（如数据库系统、应用软件、计算机网络等）的安全评估标准，可以使它们配合并适应相应的操作系统，以实现更完善的安全性能。

基于上述原因，世界各国都先后制定了相应的计算机系统的安全评估标准。



1.4.1　计算机系统的安全标准

第一个有关信息技术安全评价的标准诞生于 20 世纪 80 年代的美国。1983 年美国国防部发布了“可信计算机评估标准”，简称橘皮书。1985 年对此标准进行修订后作为了美国国防部的标准。20 世纪 90 年代，由于 Internet 技术广泛的应用，面对计算机系统安全出现的许多新问题，美国又颁布了联邦评测标准（FC）草案，用以代替 80 年代颁布的橘皮书。此外，美国还与加拿大和欧洲联合研制了 CC（信息技术安全评测通用标准）。CC 发布的目的是建立一个各国都能接受的通用安全评价准则。在欧洲，英国、荷兰和法国带头开始联合研制欧洲共同的安全评测标准，并于 1991 年颁布 ITSEC（信息技术安全标准）。1993 年，加拿大发布加拿大可信计算机产品评测标准（CTCPEC）。在安全体系结构方面，ISO 制定了国际标准 ISO7498-2-1989《信息处理系统-开放系统互连-基本参考模型第 2 部分：安全体系结构》。这些标准主要覆盖以下领域：

（1）加密标准。定义了加密的算法、加密的步骤和基本数学要求。目标是将公开数据转换为保密数据，在存储载体和公用网或专用网上使用，实现数据的隐私性和已授权人员的可读性。

（2）安全管理标准。它阐述的是安全策略、安全制度、安全守则和安全操作。旨在为一个机构提供用来制定安全标准、实施有效的安全管理时的通用要素，并使跨机构的交易得以互信。

（3）安全协议标准。协议是一个有序的过程，协议的安全漏洞可以使认证和加密的作用前功尽弃。常用的安全协议有 IP 的安全协议、可移动通信的安全协议等。

（4）安全防护标准。它的内容包括防入侵、防病毒、防辐射、防干扰和物理隔离。也包括存取访问、远程调用、用户下载等方面。

（5）身份认证标准。身份认证是信息和网络安全的首关，它也同访问授权和访问权限相连。身份认证还包括数字签名标准、数字标准、眼睛识别标准等。

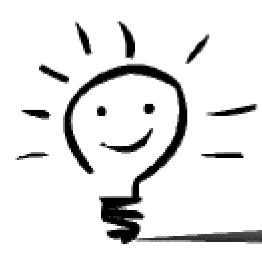
（6）数据验证标准。包括数据保密压缩、数字签名、数据正确性和完整性的验证。

（7）安全评价标准。其任务是提供安全服务与有关机制的一般描述，确定可以提供这些服务与机制的位置。

（8）安全审计标准。包括对涉及安全事件的记录、日志和审计，对攻击和违规事件的探测、记录、收集和控制。

1994 年，国务院发布了《中华人民共和国计算机信息系统安全保护条例》，其中第九条规定“计算机信息系统实行安全等级保护。安全等级的划分标准和安全等级保护的具体办法，由公安部会同有关部门制定”。公安部在《中华人民共和国计算机信息系统安全保护条例》发布实施后便着手开始了计算机信息系统安全等级保护的研究和准备工作。等级管理的思想和方法具有科学、合理、规范以及便于理解、掌握和运用等优点。因此，对计算机信息系统实行安全等级保护制度，是我国计算机信息系统安全保护工作的重要发展思想，对于正在发展中的信息系统安全保护工作更有着十分重要的意义。

目前，计算机系统安全评价标准的一个发展趋势是建立最基本、最稳定的和最经济的



操作系统评价标准，在此基础上再制定其他系统的安全评价标准。世界各国也正在为安全标准的完善进行广泛的接触和交流，并使其有了逐渐统一的趋势。

1.4.2 计算机系统的安全等级

常见的计算机系统安全等级划分有两种：一种是美国国防部 1985 年发表的评估计算机系统安全等级的“橘皮书”，将计算机系统的安全划分为 4 类 7 级，即 A、B3、B2、B1、C2、C1、D；另一种是依据我国颁布的《计算机信息系统安全保护等级划分准则》（GB17859-1999），该准则是计算机信息系统安全保护的法律基础，依据该准则将计算机安全等级划分为 5 级。

1. “橘皮书”的计算机系统安全等级

橘皮书将计算机安全归结为主体（如用户）对客体（如数据）访问时是否符合预定的安全策略，如果符合计算机系统就为安全，如能绕过控制则为不安全。在这一思想的指导下，人们将计算机系统安全的研究集中于研制实现最完善安全策略的控制器，并将计算机安全等级划分为 4 类 7 级，即 D、C、B、A 级，安全级别由低到高。D 级暂时不分子级；C 级分为 C1 和 C2 两个子级，C2 比 C1 提供更多的保护；B 级分为 B1、B2、B3 3 个子级，安全级别也是由低到高；A 级暂时不分子级。每级包括它下级的所有特性。

（1）D 级（非保护级）。

这是可用的最低安全形式。该标准说明整个计算机系统是不可信任的，对于硬件来说，没有任何保护可用；操作系统很容易被侵袭。D 级计算机系统标准规定对用户没有验证，也就是任何人都可以自由地使用该计算机系统。系统不要求用户进行登记（如要求用户提供用户名）或口令保护（如要求用户提供唯一字符串来进行访问）。D 级的计算机操作系统包括 MS-DOS、Windows 3.x、Windows 95 以及 Apple 的 System 7.x。

（2）C1 级。

C1 级也称自主安全保护系统，系统对硬件要求有某种程度的保护（如硬件带锁装置和需要钥匙才能使用计算机等），用户必须登录到系统让系统识别他们。C1 级系统还要求具有完全访问控制的能力，应当允许系统管理员为一些程序或数据设立访问许可权限 C1 级防护的不足之处在于用户可直接访问操作系统的根，不能阻止系统账户执行活动。

（3）C2 级。

C2 级也称可控安全保护级，解决了 C1 级的某些不足之处并加强了几个安全特征。C2 级具有进一步限制用户执行某些命令或访问某些文件的能力，这不仅基于许可权限，而且基于身份验证级别。使用附加身份验证，对于一个 C2 系统的用户来说，没有根口令而有权执行系统管理任务是可能的。这使得追踪与系统管理有关的任务有了改观，因为是单独的用户执行了工作而不是系统管理员。

另外，这种安全级别要求对系统加以审核，包括为系统中发生的每个事件编写一个审核记录，用来跟踪记录与安全有关的所有事件。常见的 C2 级操作系统有 UNIX、XENIX、Novell 3.x 或更高版本、Windows 2000。



（4）B1 级。

B1 级也称标记安全保护级系统，支持多级安全，多级是指这一安全保护安装在不同级别的系统中（如网络、应用程序、工作站等），它对敏感信息提供更高级的保护。例如安全级别可以分为解密、保密和绝密级别。

（5）B2 级。

这一级别也称为结构化的保护。B2 级安全要求计算机系统中所有对象加标签，而且给设备（如工作站、终端和磁盘驱动器）分配安全级别。如用户可以访问一台工作站，但可能不允许访问含有重要资料的子系统。

（6）B3 级。

B3 也称强制安全区域级，系统使用安装硬件的办法来加强域，如内存管理硬件用于保护安全域免受无授权访问或其他安全域对象的修改。该级别也要求用户终端通过一条可信任途径连接到系统上。其主要特征是高抗渗透能力，可信恢复用于绝密、机密信息的保护，即使系统崩溃，信息也不会泄密。

（7）A 级。

也称验证设计级，这是橘皮书中的最高安全级别。这一级除了包括它下面各级的所有特性，还附加一个安全系统受监视的设计要求，合格的安全个体必须分析并通过这一设计。另外，必须采用严格的形式化方法来证明该系统的安全性。而且在 A 级，所有构成系统的部件的来源必须有安全保证，这些安全措施还必须担保在销售过程中这些部件不受损害。例如，在 A 级设置中，一个磁带驱动器从生产厂房直至计算机机房都被严密跟踪。A 级安全系统用于绝密级信息的保护。

美国的计算机安全等级评估标准虽然非常盛行，但它只是着重规定了某些操作系统的安全等级，而作为一个综合的评估标准还显得不完善。

2. 我国的计算机系统安全等级

实践证明，信息技术标准化是搞好信息系统建设的重要基础工作之一，也是推广和普及信息技术的基本前提。

从 2001 年 1 月 1 日起，我国实施强制性国家标准《计算机信息安全保护等级划分准则》。该准则是建立安全等级保护制度、实施安全等级管理的重要基础性标准。它将计算机信息系统安全保护等级划分为 5 个等级，从低到高依次是用户自主保护级、系统审计保护级、安全标记保护级、结构化保护级和访问验证保护级。

（1）用户自主保护级。

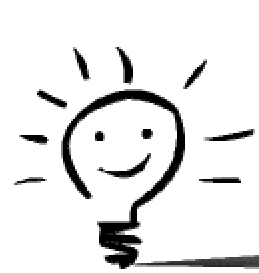
本级的安全保护机制通过隔离用户与数据，使用户具备自主安全保护能力，保护用户和用户组信息，避免其他用户对数据的非法读写和破坏。

（2）系统审计保护级。

本级的安全保护机制除具备第一级的所有安全保护功能外，还要求创建和维护访问的审计跟踪记录，使所有用户对自己行为的合法性负责。

（3）安全标记保护级。

本级的安全保护机制有系统审计保护级的所有功能，并为访问者和访问对象指定安全标记，以访问对象标记的安全级别限制访问者的访问权限，实现对访问对象的强制保护。



（4）结构化保护级。

本级安全机制具备第三级的所有安全功能，并将安全保护机制划分成关键部分和非关键部分相结合的结构，其中关键部分直接控制访问者对访问对象的存取。本级具有相当强的抗渗透能力。

（5）访问验证保护级。

本级的安全保护机制具备第四级的所有功能，并特别增设访问验证功能，负责仲裁访问者对访问对象的所有访问活动。具有极强的抗渗透能力。

《计算机信息系统安全保护等级划分准则》就是要从安全整体上进行保护，从整体上、根本上、基础上来解决等级保护问题。要建立良好的国家整体保护制度，标准体系是基础。

《计算机信息系统安全保护等级划分准则》的配套标准分为两类：一是《计算机信息系统安全保护等级划分准则应用指南》，它包括技术指南、建设指南和管理指南；二是《计算机信息系统安全保护等级评估标准》，它包括安全操作系统、安全数据库、网关、防火墙、路由器和身份认证管理等。目前，国家正在组织有关单位完善信息系统安全保护制度的标准。

本 章 小 结

计算机网络安全是指保持网络中的硬件、软件系统正常运行，使它们不因各种因素受到破坏、更改和泄露。网络受到的威胁来自于网络的内部和外部两个方面。

为实现开放系统互联网环境下的信息安全，ISO7498-2 国际标准描述了实现 OSI 参考模型之间的安全通信所必需提供的安全服务和安全机制。

计算机系统的安全评估是对系统安全性的检验和监督。在我国，常见的计算机系统安全等级的划分有两种：一种是依据美国国防部发表的评估计算机系统安全等级的橘皮书，将计算机安全等级划分为 4 类 7 级；一种是我国颁布的《计算机信息系统安全保护等级划分准则》，将计算机安全等级划分为 5 级。

习　　题

一、填空题

1．计算机网络安全是指保持网络中的硬件、软件系统正常运行，使它们不因各种因素受到________、________和________。

2．一个安全的网络体系至少应包括 3 类措施：________、________、________。

3．网络安全主要包括________、________、________和运行安全 4 个方面。

4．一个安全的网络具有 5 个特征：________、________、________、________、________。

5．网络的安全机制包括________、________、________、________、________、________、________和________。



6．依据美国国防部发表的评估计算机系统安全等级的“橘皮书”，将计算机安全等级划分为________类________级。

二、选择题

1．保护计算机网络设备免受环境事故的影响属于信息安全的________。

A．人员安全　　B．物理安全　　C．数据安全　　D．操作安全

2．在以下人为的恶意攻击行为中，属于主动攻击的是________。

A．身份假冒　　B．数据窃听　　C．数据流分析　　D．非法访问

3．有些计算机系统的安全性不高，不对用户进行验证，这类系统安全级别是________。

A．D　　B．A　　C．C1　　D．C2

4．保证数据的完整性就是________。

A．保证网络上传送的数据信息不被第三方监视

B．保证网络上传送的数据信息不被篡改

C．保证电子商务交易各方的真实身份

D．保证发送方不抵赖曾经发送过某数据信息

5．某种网络安全威胁是通过非法手段取得对数据的使用权，并对数据进行恶意地添加和修改，这种安全威胁属于________。

A．窃听数据　　B．破坏数据完整性

C．拒绝服务　　D．物理安全威胁

6．在网络安全中，捏造是指未授权的实体向系统中插入伪造的对象。这是对_______。

A．可用性的攻击　　B．保密性的攻击

C．完整性的攻击　　D．不可抵赖性的攻击

三、简答题

1．什么是网络安全？网络安全包括哪些方面？

2．网络系统本身存在哪些安全漏洞？

3．网络面临的威胁有哪些？

4．常用的网络安全技术有哪些？

5．网络的安全服务有哪些？安全机制有哪些？

本 章 实 训

实训　使用扫描工具 X-Scan 检测系统漏洞

实训目的

（1）掌握扫描工具 X-Scan 的使用方法。



（2）掌握使用扫描工具对计算机系统进行安全漏洞扫描的方法。

实训环境

（1）连上 Internet 的主机或局域网主机。

（2）Windows XP/2000/2003 系统。

操作环境

（1）连上 Internet 的主机或局域网主机。

（2）Windows NT/2000/XP 系统。

（3）X-Scan v3.3 扫描器。

操作步骤

第 1 步：运行 X-Scan 主程序，即可打开其操作窗口，如图 1.1 所示。

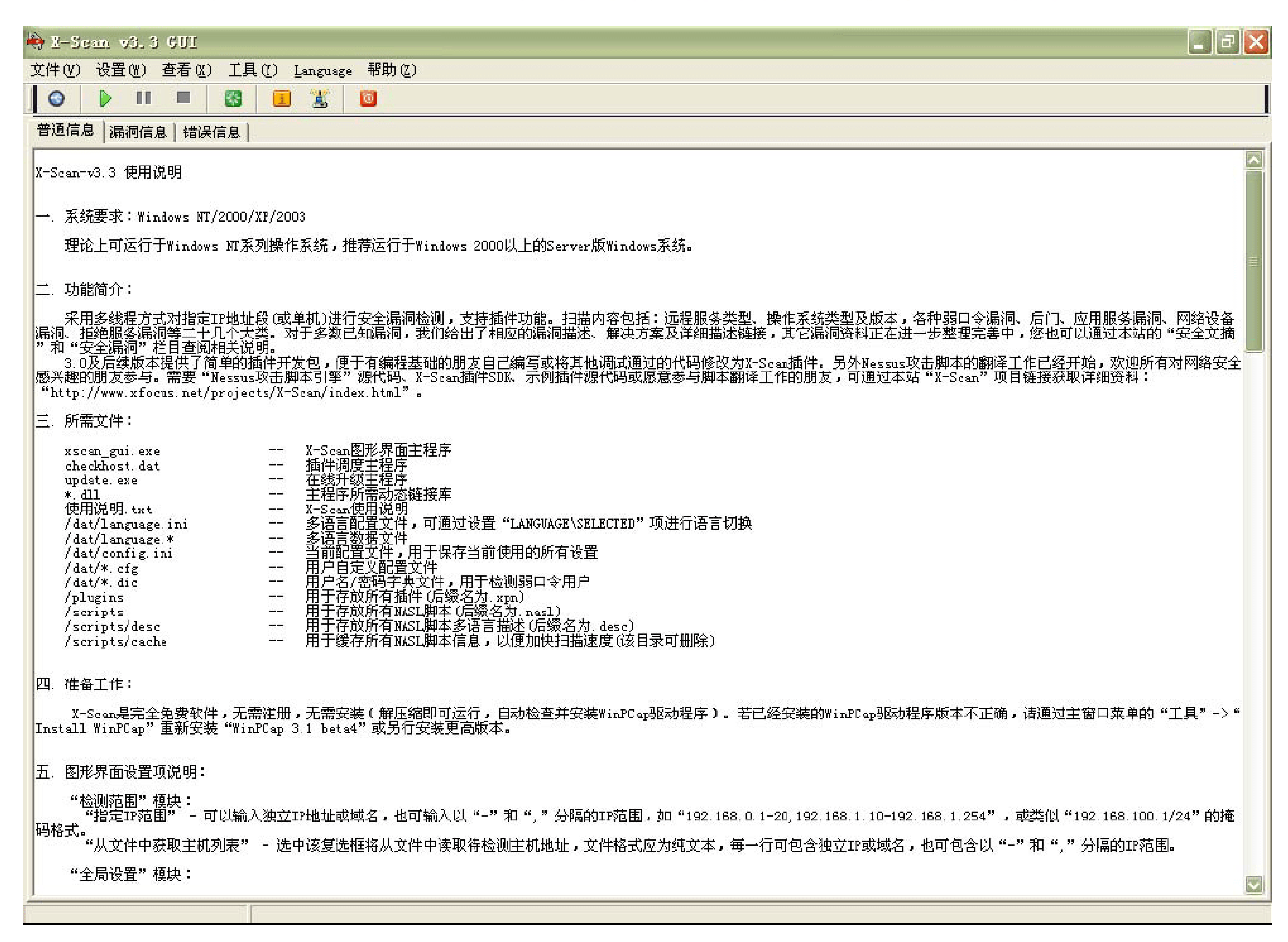


图 1.1　X-Scan 主窗口

第 2 步：执行“设置”→“扫描参数”命令，即可打开“扫描参数”窗口。在“检测范围”模块的“指定 IP 范围”文本框中，输入要检测的目标主机的域名或 IP 地址，也可以同时对多个 IP 进行检测（如输入“192.168.0.1～192.168.0.255”来对处于这个网段的所有主机进行检测），如图 1.2 所示。

第 3 步：在“全局设置”模块中，可以对要扫描的模块、端口等进行设置。“扫描模块”选项用于检测对方主机的一些服务和端口等情况，可以全部选择或只检测部分服务，如图 1.3 所示。“并发扫描”选项用于设置检测时的最大并发主机和并发线程的数量。“扫描报告”选项用于设置扫描结束所产生的报告文件名和类型。这里假设选择 HTML 类型，如图 1.4 所示。

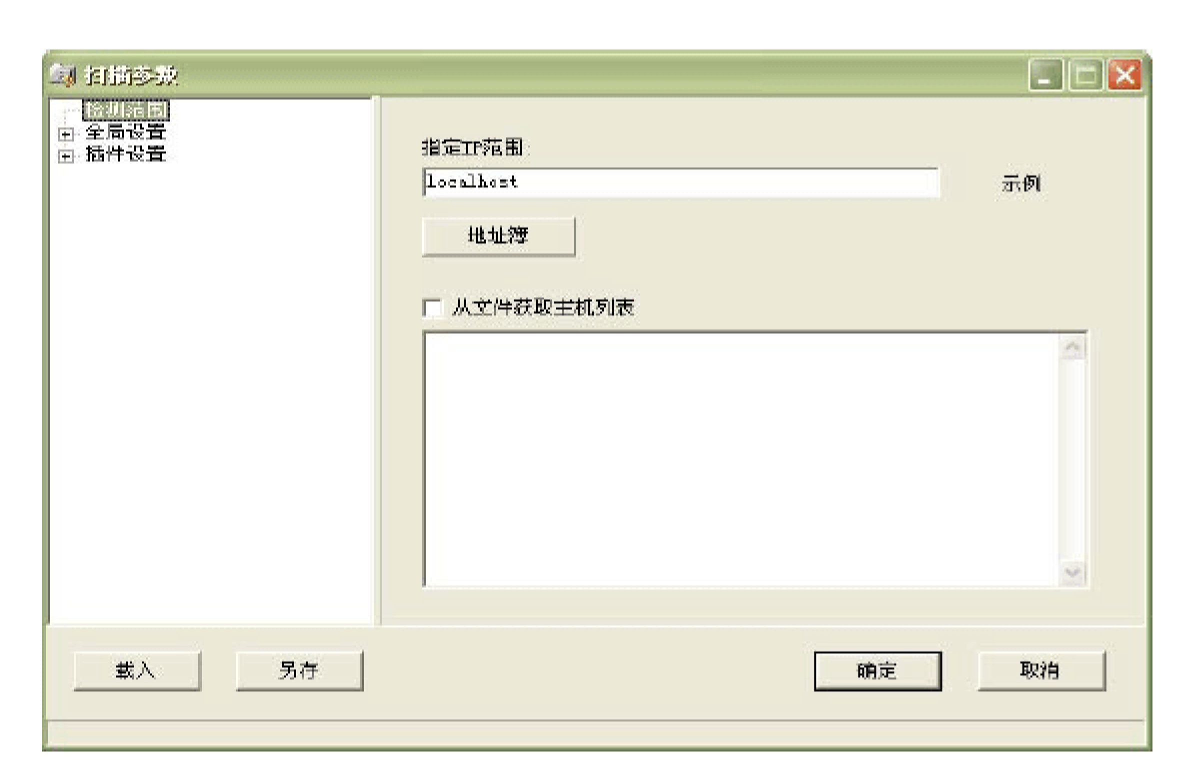


图 1.2　“扫描参数”窗口

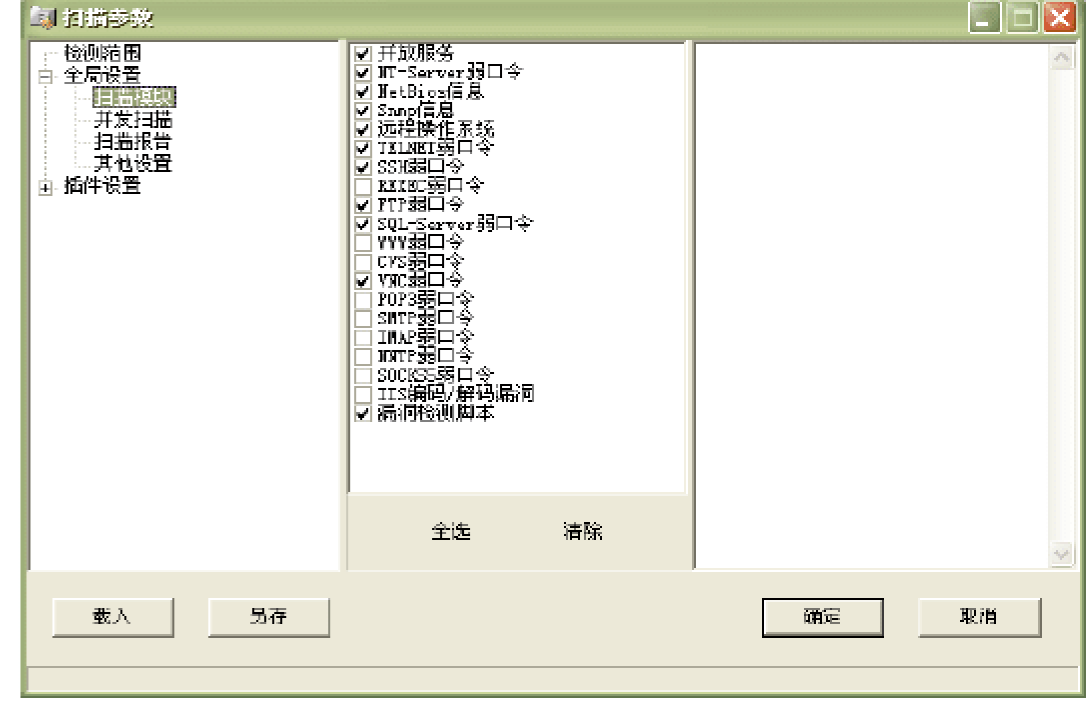


图 1.3　“扫描模块”设置

在“其他设置”选项中可设置“跳过没有响应的主机”功能，如图 1.5 所示。如果对方禁止了 Ping 操作或防火墙设置使其没有响应，则 X-Scan 将会自动跳过，接着检测下一台主机。如果选中“无条件扫描”单选按钮，则 X-Scan 将会对目标主机进行详细检测，得到的结果相对详细准确，但扫描时间会延长，对单个主机进行扫描一般会采用这种方式。

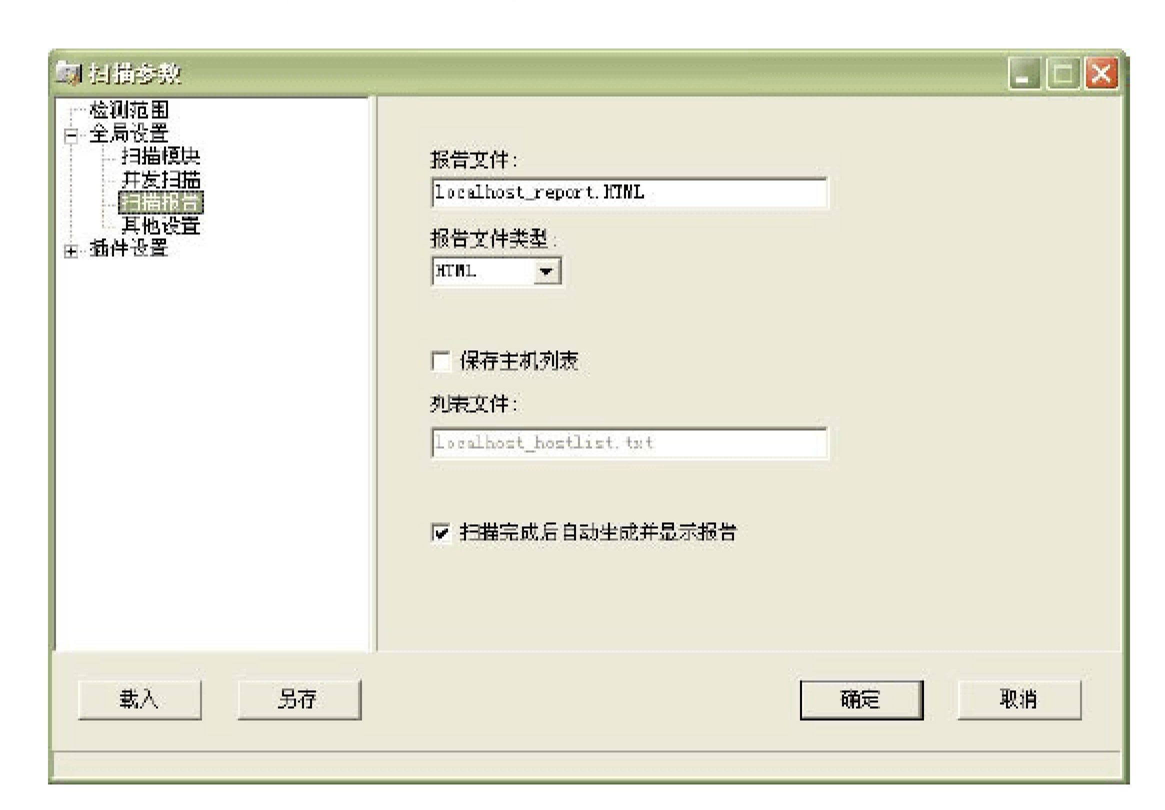


图 1.4　“扫描报告”设置

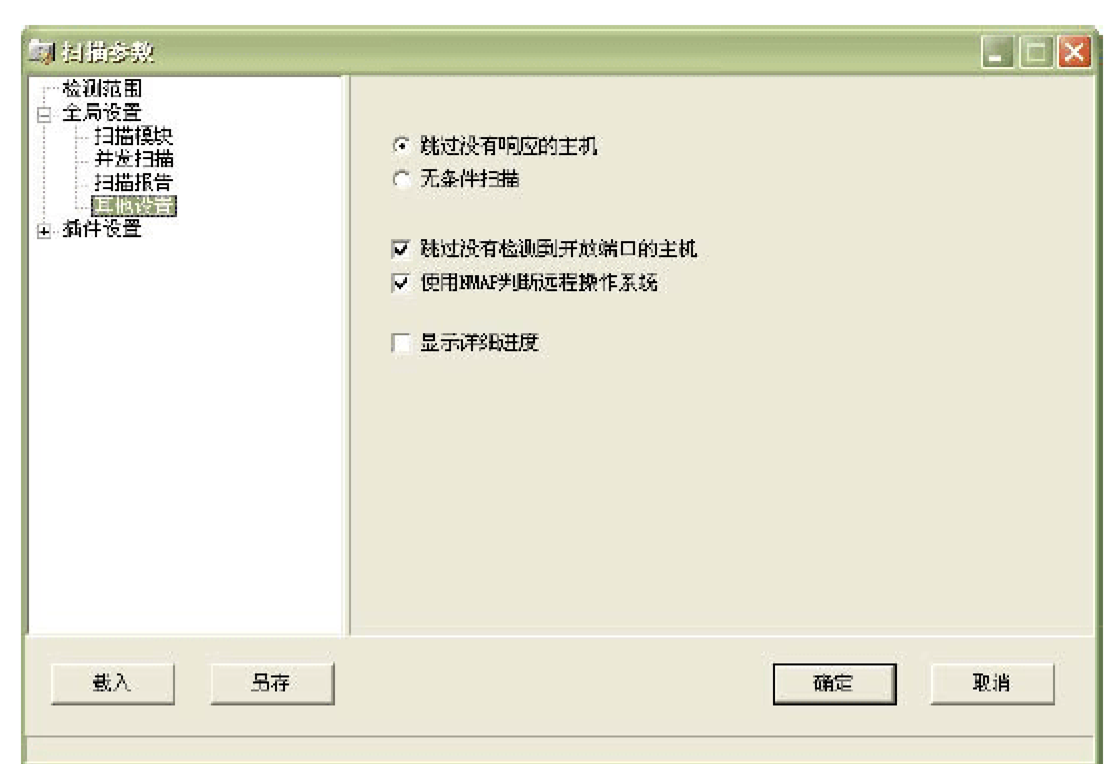


图 1.5　“其他设置”设置

第 4 步：在“插件设置”模块中，可以对插件进行一些必要的检测。

在“端口相关设置”选项中可自定义一些需要检测的端口，检测方式分 TCP 或 SYN 两种，TCP 方式容易被对方发现，但准确性要高一些；SYN 则相反，如图 1.6 所示。

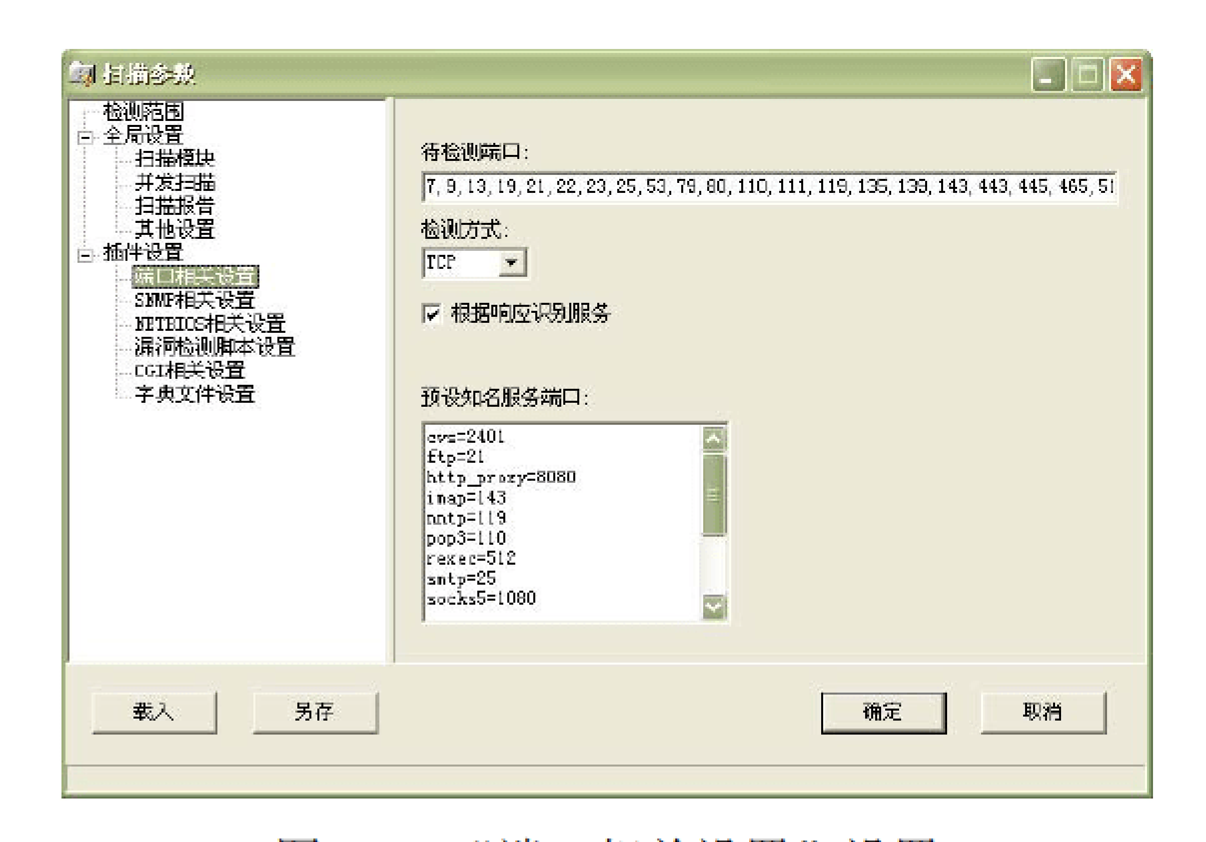


图 1.6　“端口相关设置”设置

“SNMP 相关设置”选项主要是针对 SNMP 信息的一些检测设置。“NETBIOS 相关设置”选项是针对 Windows 系统 NETBIOS 信息的检测设置，包括的项目有很多，只需要选择使用的内容即可。“漏洞检测脚本设置”、“CGI 相关设置”和“字典文件设置”等选项直接采用默认设置就可以了。

第 5 步：在设置好上述模块后，返回到 X-Scan 主窗口中单击“开始”按钮，即可出现

一个如图 1.7 所示的加载漏洞进度提示框。

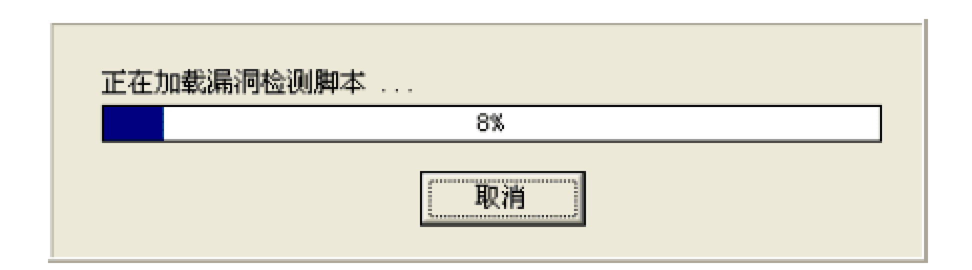


图 1.7　加载漏洞脚本提示框

第 6 步：当漏洞脚本加载完毕后，就可以进行漏洞检测了，具体检测过程如图 1.8 所示。如果检测到了漏洞，则可以在“漏洞信息”选项卡下对其进行查看。

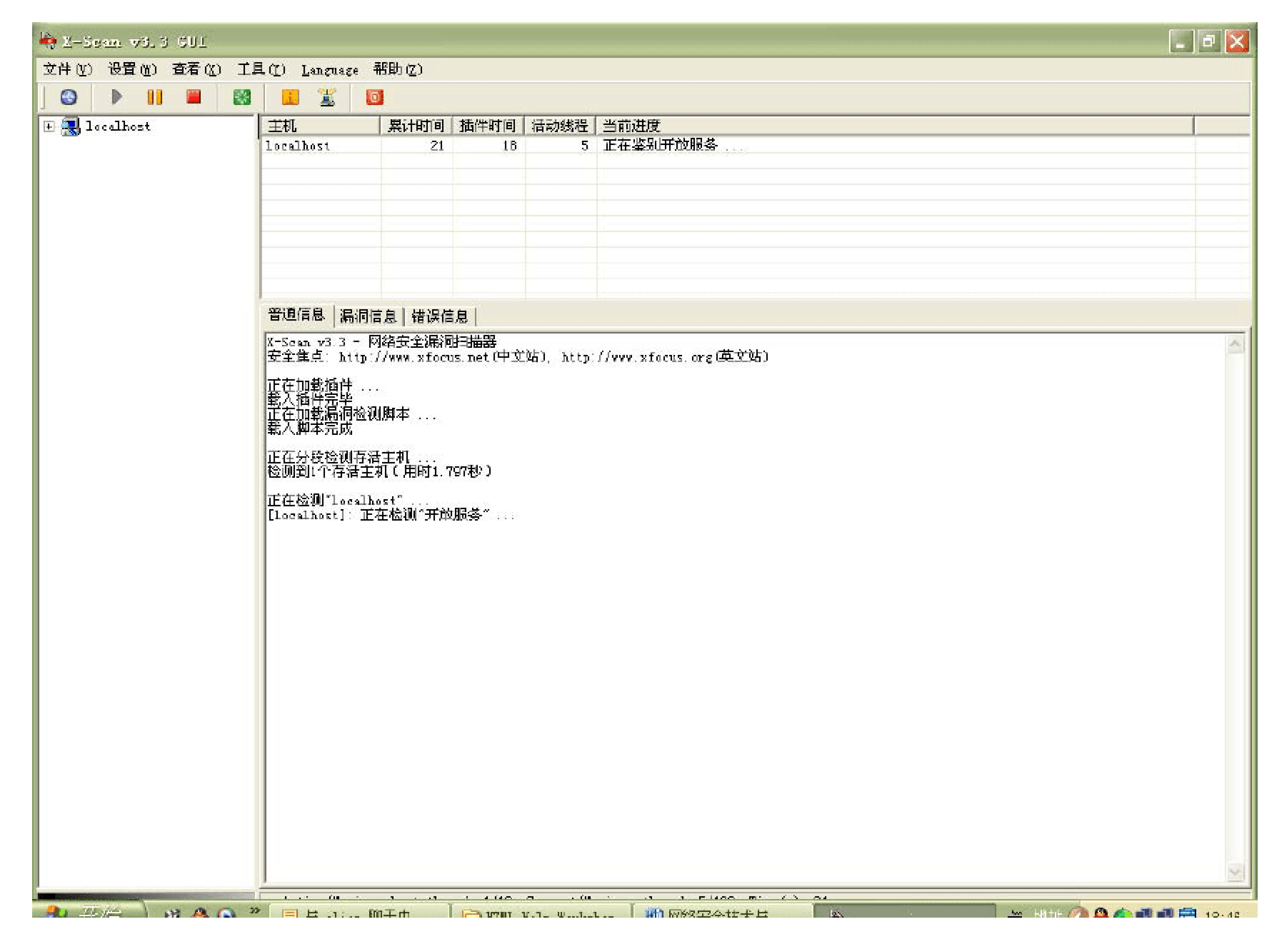


图 1.8　漏洞检测过程

第 7 步：在扫描结束后，将自动弹出漏洞检测报告，包括漏洞的风险级别和详细的信息，以便对所扫描的主机进行分析，如图 1.9 所示。



X-Scan 检测报告

本报表列出了被检测主机的详细漏洞信息，请根据提示信息或链接内容进行相应修补。欢迎参加X-Scan脚本翻译项目

扫描时间
2008-5-2 18:46:33 - 2008-5-2 18:52:31

检测结果	
存活主机	1
漏洞数量	0
警告数量	1
提示数量	15

主机列表

主机	检测结果
localhost	发现安全警告
主机摘要 - OS: Windows XP; PORT/TCP: 25, 80, 110, 135, 445, 1025	

[返回顶部]

主机分析: localhost

主机地址	端口/服务	服务漏洞
localhost	network blackjack (1025/tcp)	发现安全提示
localhost	microsoft-ds (445/tcp)	发现安全提示
localhost	http (80/tcp)	发现安全提示
localhost	pop3 (110/tcp)	发现安全提示
localhost	smtp (25/tcp)	发现安全提示
localhost	epmap (135/tcp)	发现安全提示
localhost	netbios-ssn (139/tcp)	发现安全警告

图 1.9　漏洞检测报告



第 2 章
密码技术

知识目标

- 了解威胁数据安全的各种因素。
- 理解传统和现代的数据加密技术及其基本概念。
- 理解数字签名的概念、原理及应用。

技能目标

- 熟练使用对称加密软件加、解密信息。
- 熟练使用非对称加密软件加、解密信息。

密码学是一门古老而深奥的学科，有着悠久、灿烂的历史。最早的密码形式可以追溯到 4000 多年前，古埃及人在墓志铭中使用过的类似于象形文字的奇妙符号。从古至今，密码技术一直在社会各个领域，尤其是军事、外交、情报等部门广泛使用。在信息化社会的今天，随着计算机网络和通信技术的发展，密码技术更是得到了前所未有的重视，并迅速普及和发展起来。它已经成为计算机安全研究的一个主要方向。

2.1 密码技术简介

密码学包括两部分内容：编码学和编码分析学。编码学是通过编码技术将被保护的信息的形式改变，使得编码后的信息除了指定的接收者外其他人无法理解的一门学问，也就是加密算法的研究和设计。编码分析学是研究如何攻破一个密码系统，将被加密的信息恢复，也就是密码破译技术。这两部分内容是矛与盾的关系。密码系统包括 5 个要素：明文信息空间、密文信息空间、密钥空间、加密变换 E 和解密变换 D。图 2.1 给出了密码系统示意图。

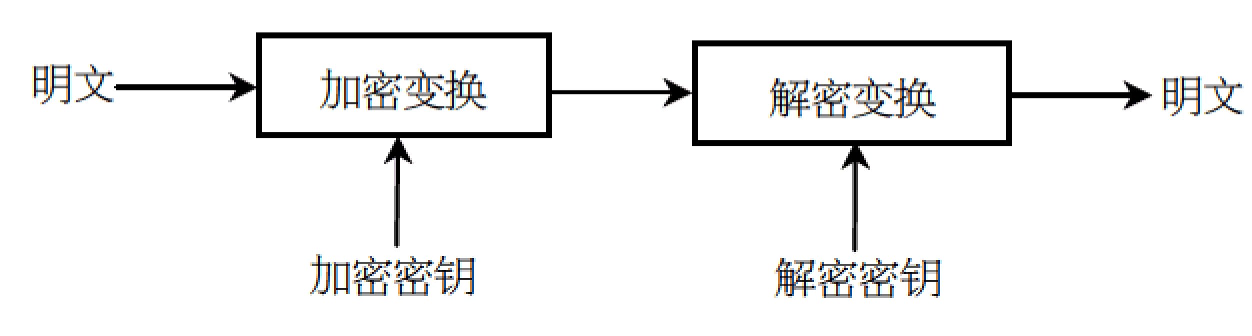


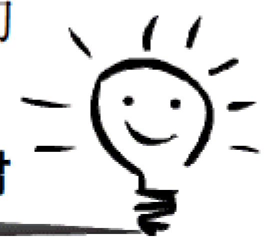
图 2.1　密码系统示意图

- ☑ 明文：加密前的原始信息。
- ☑ 密文：通过加密手段加密后的信息。
- ☑ 加密过程：将明文进行数据转换成密文的过程。
- ☑ 解密过程：利用加密的逆转换将密文恢复成明文的过程。
- ☑ 密钥：控制加密和解密运算的符号序列。

密码系统理论上要求使用方便，并且系统的保密不依赖于对加密算法和解密算法的保密，而只依赖于密钥的保密。这样，即使密文和对应的明文被截获后，仍不容易进行解密变换。

一个较为成熟的密码体系，其算法应该是公开的，而密钥是保密的。这样使用者简单地修改密钥，就可以达到改变加密过程和加密结果的目的。密钥通常是由一小串字符组成，并且可以按需要频繁更换。在加密系统的设计中，密钥的长度是一个主要的设计问题。一个 2 位数字的密钥意味着有 100 种可能性，一个 3 位数字的密钥意味着有 1000 种可能性，一个 6 位数字的密钥意味着有 100 万种可能性。密钥越长，加密系统被破译的几率就越低。

根据数据加密的方式，加密算法可以分为对称密钥加密算法（简称对称算法）和非对称密钥加密算法（简称非对称算法）两种，也称为对称数据加密技术和非对称数据加密技术。对称算法是指加密和解密的过程使用同一个密钥，它的特点是运算速度非常快，适合用于对数据本身的加解密操作。常见的对称算法有各种传统的加密算法、DES 算法等。相对于对称算法来讲，非对称算法的运算速度要慢得多，但是在多人协作或需要身份认证的



数据安全应用中，非对称算法的运算具有不可替代的作用。使用非对称算法对数据进行签名，可以证明数据发行者的身份并保证数据在传输过程中不被篡改。在这种加密算法中有两个密钥，一个称为公钥，一个称为私钥。在加密时，公钥用于加密，私钥用于解密。这种算法比较复杂，常见的非对称算法有 RSA 算法、PGP 算法等。非对称算法通常用于数据加密，由于其速度较慢，现在多采用对称算法与非对称算法相结合的加密方法，这样，既可以有很高的加密强度，也可以有较快的加密速度。此方法已广泛用于网络的数据加密传送和数字签名。通过对传输的数据进行加密来保障其安全性，已经成为了一项计算机网络系统安全的基本技术，它可以用很小的代价为数据信息提供相当大的安全保护，是一种主动的安全防御策略。

2.2　传统加密方法介绍

加密作为保障数据安全的一种方式，它不是现在才有的，它产生的历史相当久远，它的起源要追溯到公元前 2000 年了。虽然它不是现在我们所讲的加密技术，但作为一种加密的概念，确实早在几十个世纪前就诞生了。当时埃及人是最先使用特别的文字作为信息编码的，随着时间推移，巴比伦、美索不达米亚和希腊文明都开始使用一些方法来保护他们的书面信息。

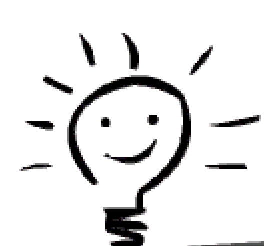
1. 替代密码

在替代密码中，用一组密文字母来代替一组明文字母以隐藏明文，但保持明文字母的位置不变。

最古老的替代密码是恺撒密码，它用 D 表示 a，用 E 表示 b，用 F 表示 c……用 C 表示 z，也就是说密文字母相对明文字母左移了 3 位。为清楚起见，一律用小写表示明文，用大写表示密文，这样明文“cipher”就变成了密文“FLSKHU”。依此类推，可以让密文字母相对明文字母左移 k 位，这样 k 就成了加密和解密的密钥。这种密码是很容易破译的，因为最多只需尝试 25 次（k=1～25）即可轻松破译密码。

较为复杂一点的密码，是明文字母和密文字母之间的映射关系，它没有规律可循，比如将 26 个英文字母随意映射到其他字母上，这种方法称为单字母表替换，其密钥是对应于所有可能的密钥，即使计算机每微秒试一个密钥，也需要 1013 年。但事实上完全不需要这么做，破译者只要拥有很少一点密文，利用自然语言的统计特征，很容易就可破译密码。破译的关键在于找各种字母或字母组合出现的频率，比如经统计发现，英文中字母 e 出现的频率最高，其次是 t、o、a、n、i 等，最常见的两字母组合依次为 th、in、er、re 和 an，最常见的三字母组合依次为 the、ing、and 和 ion。因此破译者首先可将密文中出现频率最高的字母定为 e，频率次高的字母定为 t……然后猜测最常见的两字母组、三字母组，比如密文中经常出现 tXe，就可以推测 X 很可能就是 h，如经常出现 thYt，则 Y 很可能就是 a 等。采用这种合理的推测，破译者就可以逐句组织出一个试验性的明文。

为了去除密文中字母出现的频率特征，可以使用多张密码字母表，对明文中不同位置



上的字母用不同的密码字母表来加密。比如任意选择 26 张不同的单字母密码表，相互间排定一个顺序，然后选择一个简短易记的单词或短语作为密钥，在加密一条明文时，将密钥重复写在明文的上面，则每个明文字母上的密钥字母即指出该明文字母用哪一张单字母密码表来加密。

比如要加密明文“please execute the latest scheme”，密钥为“computer”，则将“computer”重复写在报文上面，如图 2.2 所示。

c	o	m	p	u	t	e	r	c	o	m	p	u	t	…	e	r	c	o	m	p
p	l	e	a	s	e	e	x	e	c	u	t	e	t	…	s	c	h	e	m	e

图 2.2　把一段明文用密钥“computer”进行加密

于是第 1 个明文字母 p 用第 3 张（假设 a～z 分别表示顺序 1～26）单字母密码表加密，第 2 个明文字母 l 用第 12 张单字母密码表加密……显然，同一个明文字母因位置不同而在密文中可能用不同的字母来表示，从而消除了各种字母出现的频率特征。

虽然破译多字母密码表要困难一些，但如果破译者手头有较多的密文，仍然是可以破译的，破译的诀窍在于猜测密钥的长度。首先破译者假设密钥的长度，然后将密文按每行 k 个字母排成若干行，如果猜测正确，那么同一列的密文字母应是用同一单字母密码加密的，因此同一列中各密文字母的频率分布应与英文相同，即最常用的字母（对应明文字母 e）频率为 13%，次常用的字母（对应明文字母 t）频率为 9%等。如果猜测不正确，则换一个 k 进行重试，一旦猜测正确，即可逐列用破译单字母表密码的方法进行破译。进一步提高破译难度可以使用比明文更长的密钥，使上述破译方法失效，但这样的密钥难以记忆，必须记在本上，这就增加了失密的可能性。

2. 换位密码

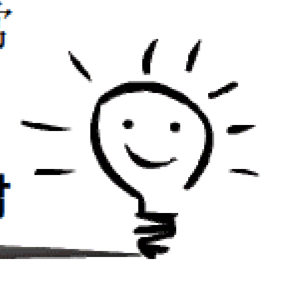
换位有时也称为排列，它不对明文字母进行变换，只是将明文字母的次序进行重新排列。图 2.3 是一种常用的换位密码，它的密钥必须是一个不含重复字母的单词或短语，加密时将明文按密钥长度截成若干行排在密钥下面，按照密钥字母在英文字母表中的先后顺序给各列进行编号，然后按照编好的序号按列输出明文即成密文。

C	O	M	P	U	T	E	R	
1	4	3	5	8	7	2	6	明文 pleaseexecutethelatestscheme
p	l	e	a	s	e	e	x	
e	c	u	t	e	t	h	e	密文 PELHEHSCEUTMLCAE ATEEXECDETTBSESA
l	a	t	e	s	t	s	e	
h	e	m	e	a	b	c	d	

图 2.3　一个换位密码的例子

破译的第一步是判断密码类型，检查密文中 E、T、O、A、N、I 等字母的出现频率，如果符合自然语言特征，则说明密文是采用换位密码加密的。

第二步是猜测密钥的长度，即列数。在许多情况下，破译者根据消息的上下文，常常



可以猜测出消息中可能包含的单词或短语，选择的单词或短语最好长一些，使其至少可能跨越两行，如“latestscheme”。将选择的单词或短语按照假定的长度 k 截成几行，由于同一列上相邻的字母在密文中必是相邻的，因此可以将各列上的各种字母组合记下来，在密文中搜索。比如将“latestscheme”按照假设的长度 8 截成两行，则相邻的字母组合有 lh、ae、tm 和 ee。假如设想的 k 是正确的，则大部分设想的字母组合在密文中都会出现，如果搜索不到，则换一个 k 再试。通过寻找各种可能性，破译者常常能够确定密钥的长度。

第三步是确定各列的顺序。如果列数比较少的话，可以逐个检查 k 个列对，查看它们的两字母组的频率是否符合英文统计特征，与特征符合最好的列对认为其位置正确。然后从剩下的列中寻找这两列的后继列，如果某列和这两列对组合后，两字母组和三字母组的频率都很好地符合英文统计特征，那么该列就是正确的后继列。通过同构法也可以找到它们的前趋列，直至最终将所有的列序全部找到。

2.3　现代加密技术介绍

2.3.1　DES 算法

数据加密标准（Data Encryption Standard，DES）是由 IBM 公司研制的加密算法，于 1977 年被美国政府采用，作为商业和非保密信息的加密标准被广泛采用。尽管该算法较复杂，但易于实现。它只对小的分组进行简单的逻辑运算，用硬件和软件实现起来都比较容易，尤其是用硬件实现使该算法的速度更快。

1. DES 算法的描述

DES 算法将信息分成 64bit 的分组，并使用 56bit 长度的密钥。它对每一个分组使用一种复杂的变位组合、替换，再进行异或运算和其他一些过程，最后生成 64 bit 的加密数据。对每一个分组进行 19 步处理，每一步的输出是下一步的输入。图 2.4 显示了 DES 算法的主要步骤。

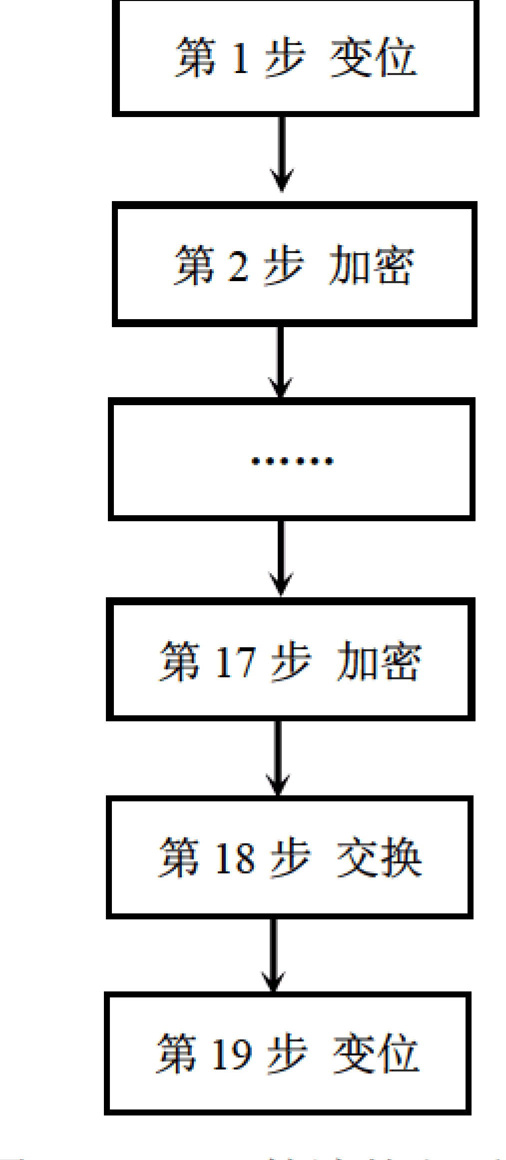


图 2.4　DES 算法的主要步骤

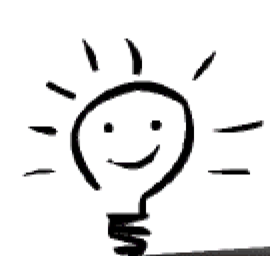
第一步对 64bit 数据和 56bit 密钥进行变位；第 2~17 步（共 16 步）除了使用源于原密钥的不同密钥外，每一步的运算过程都相同，包括很多操作；第 18 步将前 32bit 与后 32bit 交换；最后一步是第一步的逆过程，进行另一个变位。

图 2.5 显示了第 2～17 步每一步的主要操作，图中的符号说明如下。

（1）C64——64bit 的待加密的信息。

（2）K56——56bit 的密钥。

（3）L32——C64 的前 32bit。



（4）R32——C64 的后 32bit。

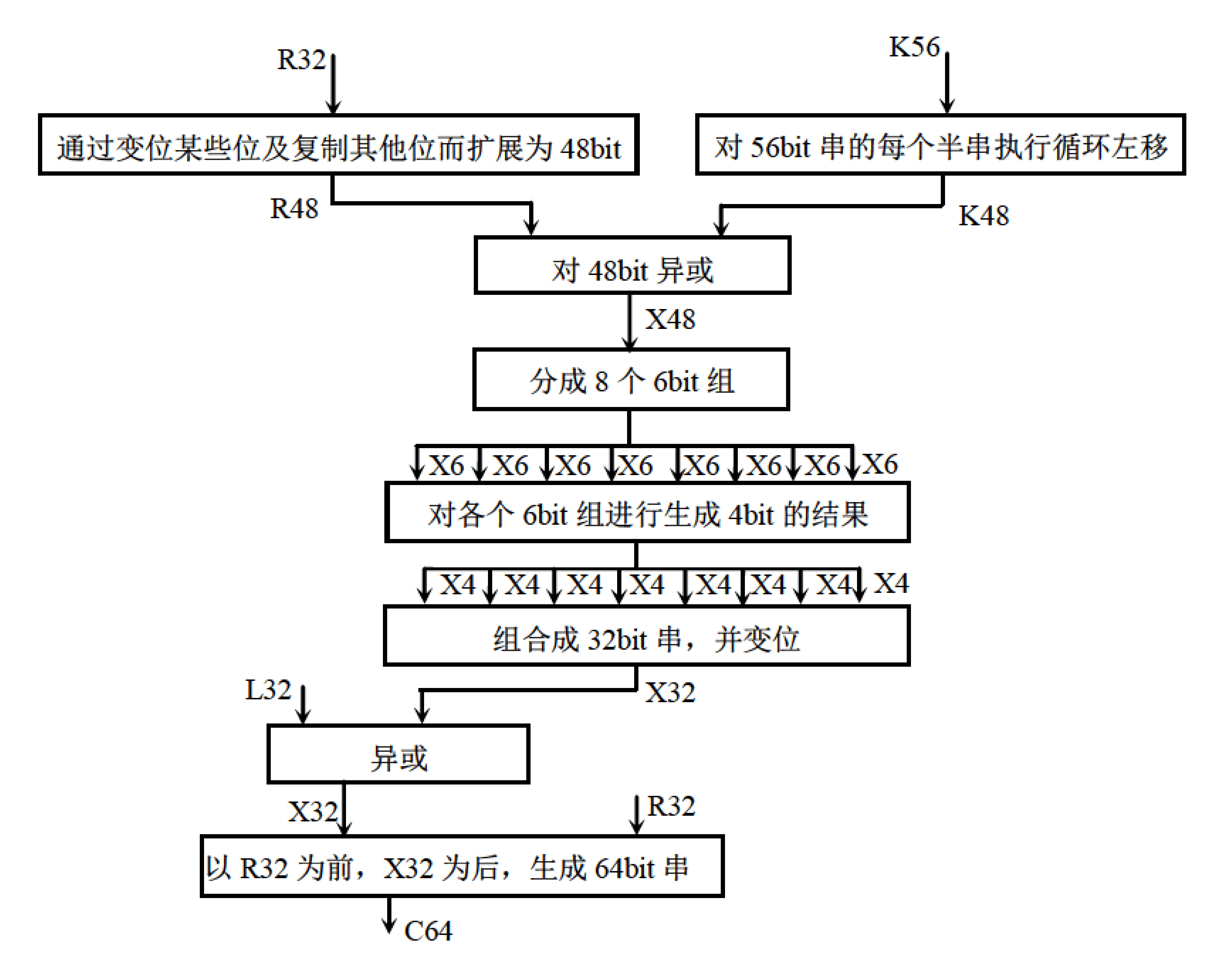


图 2.5　DES 算法的加密操作流程

（5）其他数字和字母组合中的数字都表示 bit 数，如 X48 代表处理过程中 48bit 的中间比特串。

在每一步中，密钥先移位，再从 56bit 的密钥中选出 48bit。数据后 32bit 扩展为 48bit，并与经过移位和置换的 48bit 密钥进行一次异或操作，其结果通过 8 组（每组 6bit）输出，将这 64bit 替代新的 32bit 数据，再将其变位一次，生成 32bit 串 X32。X32 与前半部分的 32bit 进行异或运算，其结果即成为新的后半部分的 32bit，原来的后半部分的 32bit 成了新的前半部分。将该操作重复 16 次，就实现了 DES 的 16 轮“加密”运算。

经过精心设计，DES 的解密和加密可使用相同的密钥和相同的算法，二者唯一的不同之处是密钥的次序相反。

2．DES 算法的安全性

DES 算法的加密和解密密钥相同，属于一种对称加密技术。对称加密技术从本质上说都是使用替代密码和换位密码进行加密的。

1977 年美国国家标准局公布了 IBM 公司研制的数据加密标准。原定该标准只使用十年，由于在这期间，该加密标准没有受到真正的威胁，因此 20 多年来一直活跃在国际保密通信的舞台上。近些年，随着计算机技术的提高，该标准已经受到现实的威胁。512bit 的密钥已经能被破解，但是要花很多的时间，计算量非常大，1024bit 长度密钥至今没能被破解。DES 作为一种高速对称加密算法，仍然具有重要意义，特别是 DES（密钥系统）和公钥系统结合组成混合密码系统。使 DES 和公钥系统（如 RSA）能够各自扬长避短，提高了加密系统的安全和效率。

3．密钥的分发与保护

DES 算法加密和解密使用相同的密钥，通信双方进行通信前必须事先约定一个密钥，这种约定密钥的过程称为密钥的分发或交换。关键是如何进行密钥的分发才能在分发的过程中对密钥保密，如果在分发过程中密钥被窃取，再长的密钥也无济于事。

最常用的一种交换密钥的方法是“难题”的使用。“难题”是一个包含潜在的密钥，必须去破解。其过程如下：

（1）发送方发送 n 个“难题”，各用不同的密钥加密。接收方并不知道解密密钥，必须去破解。

（2）接收方随机地选择一个“难题”并破解它。因为有插入在“难题”中的模式，使接收方能判断出是否破解。

（3）接收方从“难题”中抽出加密密钥，并返回给发送方一个信息指明他破解“难题”的标识号。

（4）发送方接收到接收方的返回信息后，双方即按照此“难题”的密钥进行加密了。

人们可能会问，其他人也可能截获这些“难题”，他们也可以去破解。关键是他们不知道接收方选择的难题的标识号，即便是他们又截获了接收方返回给发送方的信息，得到“难题”的标识号，但等他们破解以后，通信双方的通信过程可能已经结束了。

4．三重数据加密算法

三重数据加密算法（Three Data Encryption Algorithm，TDEA）在 1985 年第一次为金融应用进行了标准化，在 1999 年合并到数据加密标准中。

TDEA 使用 3 个密钥，按照加密→解密→加密的次序执行 3 次 DES 算法。加密、解密的过程如图 2.6 所示。

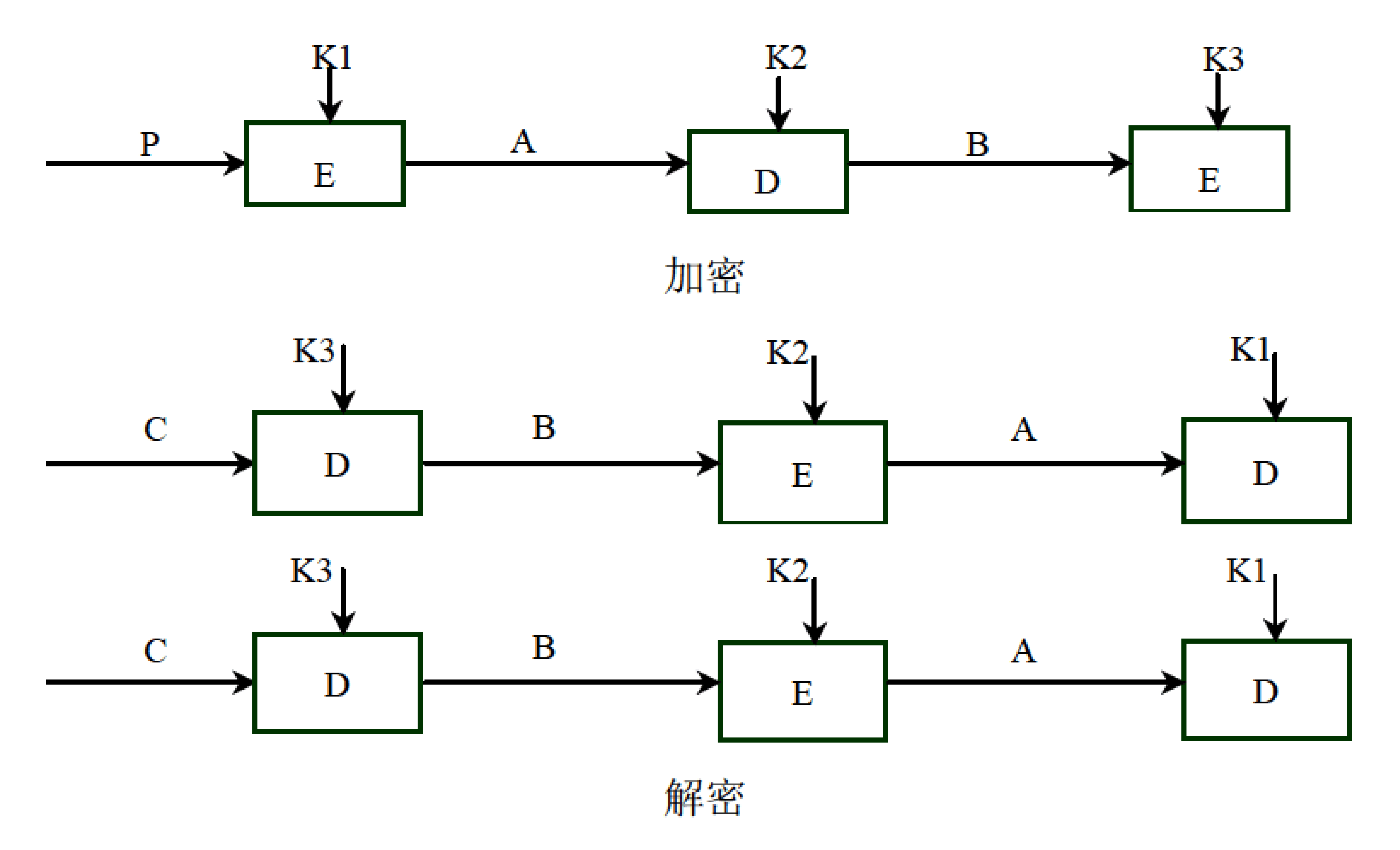


图 2.6　TDEA 加密、解密过程

图 2.6 中，P 为明文、C 为密文、E 为使用密钥 Kn 加密、D 为使用密钥 Kn 解密。

TDEA 使用 3 个不同的密钥，总有效长度为 168bit，加强了算法的安全性。



2.3.2 高级加密标准

高级加密标准（Advanced Encryption Standard，AES）又称 Rijndael 加密法，是美国联邦政府采用的一种区块加密标准。这个标准用来替代原先的 DES，已经被多方分析且广为全世界所使用。该项目于 1997 年启动，并征集算法，经过五年的甄选流程，高级加密标准由美国国家标准技术研究院（NIST）于 2001 年 11 月 26 日发布于联邦信息处理标准学报上，并在 2002 年 5 月 26 日成为有效的标准。2006 年，高级加密标准已然成为对称密钥加密中最流行的算法之一。

该算法为比利时密码学家 Joan Daemen 和 Vincent Rijmen 所设计，结合两位作者的名字，以 Rijndael 命名，投稿高级加密标准的甄选流程并胜出（Rijdael 的发音近于“Rhinedoll”）。

AES 是一个迭代的、对称密钥分组的密码，它可以使用 128bit、192bit 和 256bit 密钥，并且用 128bit（16 字节）分组加密和解密数据。与公共密钥密码使用密钥对不同，对称密钥密码使用相同的密钥加密和解密数据。通过分组密码返回的加密数据的位数与输入数据相同。迭代加密使用一个循环结构，在该循环中重复置换（permutations）和替换（substitutions）输入数据。

2.3.3 RSA 算法

公开密钥加密算法展现了密码应用中的一种崭新的思想，公开密钥加密算法采用非对称加密算法，即加密密钥和解密密钥不同。因此在采用加密技术进行通信的过程中，不仅加密算法本身可以公开，甚至加密用的密钥也可以公开（为此加密密钥也被称为公钥），而解密密钥由接收方自己保管（为此解密密钥也被称为私钥），增加了保密性。

RSA 算法是由 R.Rivest、A.Shamir 和 L.Adleman 于 1997 年提出的。RSA 的取名就来自于这 3 位发明者姓的第一个字母。后来，他们在 1982 年创办了以 RSA 命名的公司 RSA Data Sectrity Inc.和 RSA 实验室，该公司和实验室在公开密钥密码系统的研究和商业应用推广方面具有举足轻重的地位。

目前，RSA 被广泛应用于各种安全和认证领域，如 Web 服务器和浏览器信息安全、E-mail 的安全和认证、对远程登录的安全保证和各种电子信用卡系统。

RSA 算法使用模运算和大数分解，算法的部分理论基于数学中的数论。下面通过具体实例说明该算法是如何工作的。为了简化起见，在该实例中仅考虑包含大写字母的信息。实际上该算法可以推广到更大的字符集。

1. RSA 算法的加密过程

RSA 算法加密过程的具体步骤如下：

（1）为字母制定一个简单的编码，如 A～Z 分别对应 1～26。

（2）选择一个足够大的数 n，使 n 为两个大的素数（只能被 1 和自身整除的数）p 和 q 的乘积。为便于说明，在此使用 $n=p\times q=3\times 11=33$。

（3）找出一个数 k，k 与$(p-)\times(q-1)$互为素数。此例中选择 k=3，与 2×10=20 互为素数。



数字 k 就是加密密钥。根据数论中的理论，这样的数一定存在。

（4）将要发送的信息分成多个部分，一般可以将多个字母分为一部分。在此例中将每一个字母作为一部分。若信息是“SUZAN”，则分为 S、U、Z、A 和 N。

（5）对每部分，将所有字母的二进制编码串接起来，并转换成整数。在此例中各部分的整数分别为 19、21、26、1 和 14。

（6）将每个部分扩大到它的 k 次方，并使用模 n 运算，得到密文。在此例中分别是 $19^3 \bmod 33=28$，$21^3 \bmod 33=21$，$26^3 \bmod 33=20$，$1^3 \bmod 33=1$ 和 $14^3 \bmod 33=5$。接收方收到的加密信息是 28、21、20、1 和 5。

2. RSA 算法的解密过程

RSA 算法的解密过程的具体步骤如下：

（1）找出一个数 k' 使得 $(k\times k'-1) \bmod ((p-1)\times(q-1)) =0$，即 $k\times k'-1$ 能被 $(p-1)\times(q-1)$ 整除。k' 的值就是解密密钥。在此例中选择 $k'=7$，$3\times7-1=20$，$(p-1)\times(q-1)=20$，能被整除。

（2）将每个密文扩大到它的 k' 次方，并使用模 n 运算，可得到明文。在此例中分别为 $28^7 \bmod 33=19$，$21^7 \bmod 33=21$，$20^7 \bmod 33=26$，$1^7 \bmod 33=1$ 和 $5^7 \bmod 33=14$。接收方解密后得到的明文的数字是 19、21、26、1 和 14，对应的字母是 S、U、Z、A 和 N。

上述的加密和解密过程可以用表 2.1 表示。

表 2.1　RSA 加密和解密过程

发送方计算机				接收方计算机		
明　　文		P^3	密　　文	E^7	解　　密	
符　　号	数　　值		$P^3 \bmod 33$		$E^7 \bmod 33$	符　　号
S	19	6859	28	12492928512	19	S
U	21	9261	21	1801088541	21	U
Z	26	17576	20	1280000000	26	Z
A	1	1	1	1	1	A
N	14	2744	5	78125	14	N

3. RSA 算法的安全性

RSA 算法的加密过程要求 n 和 k，解密过程要求 n 和 k'。n 和 k 以及算法都是公开的。现在已知 n 和 k 的情况下是否能很容易或很快求出 k'，是衡量 RSA 算法安全性的关键因素。

在已知 n 和 k 的情况下求 k' 的关键是对 n 的因式分解，找出 n 的两个素数 p 和 q。而出于算法的安全性考虑，就必须选择大的 n，也就意味着密钥的长度要足够长。

密钥长度越大，安全性也就越高，但相应的计算机速度也就越慢。由于高速计算机的出现，以前认为已经很具有安全性的 512bit 密钥长度已经不再满足人们的需要。1997 年，RSA 组织公布当时密钥长度的标准是个人使用 768bit 密钥，公司使用 1024bit 密钥，而一些非常重要的机构使用 2048bit 密钥。

4. 对称和非对称数据加密技术的比较

对称数据加密技术和非对称数据加密技术的区别如表 2.2 所示。

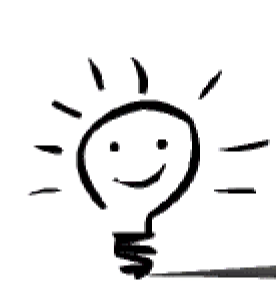


表 2.2　对称数据加密技术和非对称数据加密技术的区别

	对称数据加密技术	非对称数据加密技术
密码个数	1 个	2 个
算法速度	较快	较慢
算法对称性	对称，解密密钥可以从加密密钥中推算出来	不对称，解密密钥不能从加密密钥中推算出来
主要应用领域	数据的加密和解密	对数据进行数字签名、确认、鉴定、密钥管理和数字封装等
典型算法实例	DES 等	RSA 等

2.4　数 字 签 名

2.4.1　什么是数字签名

生活中，许多文件的真实性和可靠性最终要根据是否有亲笔签名来确定，复印件是无效的。如果要用计算机报文代替纸墨文件的传送，就必须找到数字签名来确定，这样，数字签名就应运而生了。如今，数字签名已经在诸如电子邮件、电子转账、办公室自动化等系统中大量应用了。

数字签名，就是只有信息的发送者才能产生别人无法伪造的一段数字串，这段数字串同时也是对信息的发送者发送信息真实性的一个有效证明。

数字签名是非对称密钥加密技术与数字摘要技术的应用。

数字签名文件的完整性是很容易验证的，而且数字签名具有不可抵赖性（不需要笔迹专家来验证）。

简单地说，所谓数字签名就是附加在数据单元上的一些数据，或是对数据单元所作的密码变换。这种数据或变换允许数据单元的接收者用以确认数据单元的来源和数据单元的完整性并保护数据，防止被人（如接收者）进行伪造。它是对电子形式的消息进行签名的一种方法，一个签名消息能在一个通信网络中传输。基于公钥密码体制和私钥密码体制都可以获得数字签名，主要是基于公钥密码体制的数字签名。包括普通数字签名和特殊数字签名。普通数字签名算法有 RSA、ElGamal、Fiat-Shamir、Guillou-Quisquarter、Schnorr、Ong-Schnorr- Shamir 数字签名算法、Des/DSA、椭圆曲线数字签名算法和有限自动机数字签名算法等。特殊数字签名有盲签名、代理签名、群签名、不可否认签名、公平盲签名、门限签名、具有消息恢复功能的签名等，它与具体应用环境密切相关。

数字签名的应用涉及到法律问题，美国联邦政府基于有限域上的离散对数问题制定了自己的数字签名标准（DSS）。

数字签名的主要功能是保证信息传输的完整性、发送者的身份认证，防止交易中的抵赖发生。

数字签名技术将摘要信息用发送者的私钥加密，与原文一起传送给接收者。接收者只



有用发送者的公钥才能解密被加密的摘要信息，然后用 HASH 函数对收到的原文产生一个摘要信息，与解密的摘要信息对比。如果相同，则说明收到的信息是完整的，在传输过程中没有被修改，否则说明信息被修改过，因此数字签名能够验证信息的完整性。

数字签名是个加密的过程，数字签名验证是个解密的过程。

2.4.2　数字签名的实现

数字签名可以用对称算法实现，也可以用非对称算法实现，还可以用报文摘要算法来实现。

1. 使用对称密钥密码算法进行数字签名

对称密钥密码算法所用的加密密钥和解密密钥通常是相同的，即使不同也可以很容易地由其中的一个推导出另一个。在此算法中，加、解密双方所用的密钥都要保守秘密。由于其计算速度快而广泛应用于大量数据的加密过程中。使用对称密钥密码算法进行数字签名的加密标准有 DES、RC2、RC4 等。

其签名和验证过程为利用一组长度是报文 n 的位数的两倍的密钥 A 来产生对签名的验证信息，即随机选择 $2n$ 个数 B，由签名密钥对这 $2n$ 个数 B 进行一次加密交换，得到另一组 $2n$ 个数 C。发送方从报文分组的第一位开始依次检查，若为 0 时，取密钥 A 的第 1 位，若为 1 则取密钥 A 的第 2 位……直至报文全部检查完毕。所选取的 n 个密钥位形成了最后的签名。接受方对签名进行验证时，也是首先从第 1 位开始依次检查报文分组，如果它的第 x 位为 0 时，它就认为签名中的第 x 组信息是密钥 A 的第 x 位，若为 1 则为密钥 A 的第 x+1 位，直至报文全部验证完毕，就得到了 n 个密钥。由于接收方具有发送方的验证信息 C，所以可以利用得到的 n 个密钥检验验证信息，从而确认报文是否是由发送方所发送。

由于这种方法是逐位进行签名的，所以只要有一位被改动过，接收方就得不到正确的数字签名，因此其安全性较好。其缺点是签名太长，签名密钥及相应的验证信息不能重复使用，否则极不安全。

2. 使用非对称密钥密码算法进行数字签名

非对称密钥密码算法（即公钥密码算法）使用两个密钥：公开密钥和私有密钥，分别用于数据的加密和解密，即如果用公开密钥对数据进行加密，只有用对应的私有密钥才能进行解密。如果用私有密钥对数据进行加密，则只有用对应的公开密钥才能解密。使用公钥密码算法进行数字签名的加密标准有 RSA、DSA、Diffie-Hellman 等。

其签名和验证过程为：发送方首先用公开的单向函数对报文进行一次变换，得到数字签名，然后利用私有密钥对数字签名进行加密后，附在报文之后一同发出。接收方用发送方的公开密钥对数字签名进行解密交换，得到一个数字签名的明文。发送方的公钥可以由一个可信赖的技术管理机构，即认证中心（CA）发布。接收方将得到的明文通过单向函数进行计算，同样得到一个数字签名，再将两个数字签名进行对比。如果相同，则证明签名有效，否则无效。

这种方法使任何拥有发送方公开密钥的人都可以验证数字签名的正确性。由于发送



方私有密钥的保密性，使得接收方既可以根据结果来拒收该报文，也能使其无法伪造报文签名及对报文内容进行修改，原因是数字签名是对整个报文进行的，是一组代表报文特征的定长代码，同一个人对不同的报文将产生不同的数字签名。这就解决了银行通过网络传送一张支票，而接收方可能对支票数额进行改动的问题，也避免了发送方逃避责任的可能性。

3. MD5 报文摘要算法

报文摘要是最主要的数字签名方法，也称之为数字摘要法或数字指纹法。该数字签名方法是将数字签名与要发送的信息紧密联系在一起，它更适合电子商务活动。将一个报文内容与签名结合在一起，比内容和签名分开传递，有着更强的可信度和安全性。使用报文摘要算法进行数字签名的通用加密标准有 SHA-1、MD5 等。下面以 MD5 为例简要说明。

MD5 是目前应用最广泛的报文摘要算法，可以为每个文件生成一个数字签名。MD5 属于一种 HASH 函数，其定义为：算法以一个任意长信息作为输入，产生一个 128bit 的“指纹”或“摘要信息”。

MD5 算法是对需要进行摘要处理的报文信息块按 512bit 处理的。首先它对报文信息进行填充，使其长度等于 512 的倍数。填充的方法是在需要进行摘要处理的报文信息块后填充 64B 长的信息长度，然后再用首位为 1，后面全为 0 的信息进行填充。再对信息报文进行处理，每次处理 512bit，每次进行 4 轮（每轮 16 步，共 64 步）的信息变换处理，每次输出结果为 128bit，然后把前一次的输出结果作为下一次信息变换的输入初值，这样最后输出一个 128bit 的 HASH 摘要结果。目前 MD5 被认为是最安全的 HASH 算法之一，已经在很多应用中被当成标准来使用。

MD5 提供了一种单向的 HASH 函数，是一种校验工具。它将一个任意长的字串作为输入，产生一个 128bit 的“报文摘要”，附在信息报文后面，以防报文被篡改。MD5 被认为对两个不同报文产生相同的报文摘要是不可计算的，并且对一个已给定的报文摘要，对另一个报文产生同样的报文摘要也是不可计算的。

在计算机安全中，MD5 算法是非常有效的一种对付特洛伊木马程序的工具。通过 MD5 算法计算每个文件的数字签名可以检查文件是否被更换或是否与原来一致。

2.4.3 数字签名的发展方向

1. 数字签名的不足

在实际应用中，数字签名还存在一些不足之处。

（1）数字签名亟需相关法律条文的支持。需要立法机构对数字签名技术有足够的重视，并且在立法上加快脚步，迅速制定有关法律，以充分实现数字签名具有的特殊鉴别作用，有力地推动电子商务以及其他网上事务的发展。

（2）如果发送方的信息已经进行了数字签名，那么接收方就一定要有数字签名软件，这就要求软件具有很高的普及性。

（3）假设某人发送信息后，被取消了原有数字签名的权限，以往发送的数字签名在鉴定



时只能在取消确认列表中找到原有确认信息，这样就需要鉴定中心结合时间信息进行鉴定。

（4）数字签名中的基础设施，如鉴定中心、在线存取数据库等的建设费用，可能会影响到这项技术的全面推广。

2. 数字签名的发展方向

首先，现有的一些基于优良算法的数字签名还会有很大的发展，如基于大整数因子分解难题的 RSA 算法和基于椭圆曲线上离散对数计算难题的 ECC 算法等。

随着加密、生成和验证数字签名的工具的不断完善，会建立广泛的协作机制来支持数字签名，这将是 Web 发展的目标。确保数据保密性、数据完整性和不可否认性才能保证电子商务的安全交易。今后，与数字签名有关的复杂认证能力将像现在应用环境中的口令保护一样，直接做到操作系统环境、信息传递系统及 Internet 防火墙。

数字签名作为电子商务的应用技术，将越来越受到人们的重视。其中涉及到的关键技术也很多，并且有很多新的协议，如网上交易安全协议 SSL、SET 都会涉及到数字签名，究竟使用哪种算法、哪种 HASH 函数以及数字签名管理，在通信实体与可能有的第三方之间使用协议等问题都可以作为新的课题。相信，数字签名的前景将越来越广阔。

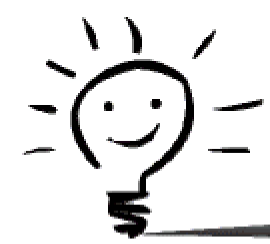
2.5　密 钥 管 理

由于加密算法的分开，对明文的保密将主要依赖于密钥。一旦密钥丢失或出错，不仅合法用户不能提取信息，而且可能会导致非法用户窃取信息。所以，密钥的安全管理在信息系统安全中是极为重要的。它不仅会影响系统的安全性，还会涉及到系统的可靠性、有效性和经济性。

密钥管理包括密钥的产生、存储、装入、分配、保护、丢失、销毁等内容。其方法的选取是基于参与者对使用该方法的环境所作的评估之上。对环境的考虑包括要进行防范所使用的技术、提供的密码服务的体系结构与定位，以及密码服务提供者的物理结构与定位。

1. 对称密钥管理

对称加密是基于共同保守秘密来实现的。采用对称加密技术的贸易双方必须要保证采用的是相同的密钥，要保证彼此密钥的交换是安全可靠的，同时还要设定防止密钥泄密和更改密钥的程序。这样，对称密钥的管理和分发工作将变成一件潜在危险的和繁琐的过程。通过公开密钥加密技术实现对称密钥的管理使相应的管理变得简单和更加安全，同时还解决了纯对称密钥模式中存在的可靠性问题和鉴别问题。贸易方可以为每次交换的信息（如每次的 EDI 交换）生成唯一一个对称密钥并用公开密钥对该密钥进行加密，然后再将加密后的密钥和用该密钥加密的信息（如 EDI 交换）一起发送给相应的贸易方。由于每次信息交换都对应生成了唯一一个密钥，因此各贸易方就不再需要对密钥进行维护和担心密钥的泄露或过期。这种方式的另一优点是，即使泄露了一个密钥也只将影响一笔交易，而不会影响到贸易双方之间所



有的交易关系。这种方式还提供了贸易伙伴间发布对称密钥的一种安全途径。

2. 公开密钥管理/数字证书

贸易伙伴间可以使用数字证书（公开密钥证书）来交换公开密钥。国际电信联盟（ITU）制定的标准 X.509 对数字证书进行了定义，该标准等同于国际标准化组织（ISO）与国际电工委员会（IEC）联合发布的 ISO/IEC 9594-8：195 标准。数字证书通常包含有唯一标识证书所有者（即贸易方）的名称、唯一标识证书发布者的名称、证书所有者的公开密钥、证书发布者的数字签名、证书的有效期及证书的序列号等。证书发布者一般称为证书管理机构（CA），它是贸易各方都信赖的机构。数字证书能够起到标识贸易方的作用，是目前电子商务广泛采用的技术之一。

3. 密钥管理相关的标准规范

目前国际有关的标准化机构都在着手制定关于密钥管理的技术标准规范。ISO 与 IEC 下属的信息技术委员会（JTC1）已起草了关于密钥管理的国际标准规范。该规范主要由 3 部分组成：一是密钥管理框架；二是采用对称技术的机制；三是采用非对称技术的机制。该规范现已进入到国际标准草案表决阶段，并将很快成为正式的国际标准。

2.6 非对称加密软件 PGP

PGP（Pretty Good Privacy）是一种操作简单、使用方便、普及程度较高的基于非对称加密算法 RSA 公钥体系的邮件加密软件。PGP 不但可以对电子邮件加密，防止非授权者阅读信件，还能对电子邮件附加数字签名，使收信人能明确了解发信人的真实身份，也可以在不需要通过任何保密渠道传递密钥的情况下，使人们安全地进行保密通信。

PGP 创造性地把 RSA 非对称加密算法的方便性和传统加密体系结合起来，在数字签名和密钥认证管理机制方面采用了无缝结合的巧妙设计，同时具有良好的人机工程设计。它功能强大，有很快的速度，而且是完全免费的。另外，PGP 还可以用来加密各种类型的文件，这些使其几乎成为最为流行的公钥加密软件包。

PGP 实际上是采用 IDEA 传统加密算法来加密的，而不是 RSA 本身。原因是 RSA 算法计算量极大，在速度上不适合加密大量数据，而 IDEA 的加解密速度比 RSA 要快得多，所以实际上 PGP 是以一个随机生成的密钥，用 IDEA 算法对明文加密，然后再用 RSA 算法对该密钥进行加密。收件人同样是用 RSA 解密出这个随机密钥，再用 IDEA 解密邮件本身。这样的链式加密就做到了既有 RSA 体系的保密性，又有 IDEA 算法的快捷性。

用 PGP 进行数字签名的过程为：发送方用自己的私钥将 128bit 的特征值加密，附加在电子邮件后，再用接收方的公钥将整个邮件加密。在这里特别要注意次序，如果先加密再签名的话，别人可以将签名去掉后加上自己的签名，从而篡改签名。密文收到以后，接收方用自己的私钥将邮件解密，得到发送方的原文和签名，然后用 PGP 从原文计算出一个 128bit 的特征值来和用发送方的公钥解密签名所得到的数进行比较，如果符合就说明这份邮件确实是发送方寄来的。这样就使两个安全性要求都得到了解决。

PGP 还可以只签名而不加密，这适用于公开发表声明时，声明人为了证实自己的身份，可以用自己的私钥签名。这样就可以让收件人能确认发信人的身份，也可以防止发信人抵赖自己的声明。这一点在商业领域有很大的应用前途，它可以防止发信人抵赖和信件被中途篡改。

本 章 小 结

加密技术是保护数据安全的一种最常用的技术。数据加密技术分为两种：传统加密方法和现代加密方法。传统加密方法的典型代表是替代密码和换位密码技术。现代加密方法的典型代表是 RSA 和 DES 加密方法。

数字签名是加密技术的典型应用，用来保证信息传输过程中信息的完整性和提供信息发送者的身份认证。

习　　题

一、填空题

1．DES 使用的密钥长度是________位。

2．AES 可以使用________、________和________位密钥，并且用________位分组加密和解密数据。

2．有一类加密类型通常用于数据完整性检验和身份验证，例如计算机系统中的口令就是利用________算法加密的。

3．认证技术主要解决网络通信进程中通信双方________认可。

4．电子商务中的数字签名通常利用公开密钥加密方法实现，其中发送者签名使用的密钥为发送者的________。

5．数字签名是用于确认发送者身份和消息完整性的一个加密的________。

二、选择题

1．如果使用恺撒密码，在密钥为 4 时 attack 的密文为________。

A．ATTACK　　B．DWWDFN　　C．EXXEGO　　D．FQQFAO

2．按密钥的使用个数，密码系统可以分为________。

A．置换密码系统和易位密码系统　　B．分组密码系统和序列密码系统

C．对称密码系统和非对称密码系统　　D．密码学系统和密码分析学系统

3．计算机网络系统中广泛使用的 DES 算法属于________。

A．非对称加密　　B．对称加密　　C．不可逆加密　　D．公开密钥加密

4．在公钥密码体系中，下面______是可以公开的。

I．加密算法　　II．公钥　　III．私钥

A．仅 I　　B．仅 II　　C．仅 I 和 II　　D．全部

5．关于数字签名，下面说法错误的是________。

A．数字签名技术能够保证信息传输过程中的安全性

B．数字签名技术能够保证信息传输过程中的完整性

C．数字签名技术能够对发送者的身份进行认证

D．数字签名技术能够防止交易中抵赖的发生

三、简答题

1．简述密码技术的概念。

2．简要描述传统的加密方法。

3．公开密钥体制 RSA 算法的主要特点是什么？

4．说明数字签名实现的过程。

5．怎样进行密钥的管理？

本 章 实 训

实训 1　使用 Apocalypso 加密软件加、解密文件

实训目的

（1）了解对称加密技术的基本原理。

（2）熟练使用 Apocalypso 加密软件加、解密文件。

实训环境

Windows XP/2000/2003 操作系统，Apocalypso 加密软件。

操作步骤

第 1 步：在桌面上创建一个文本文件，取名为 text.txt，并输入文字“对称加密实验”，如图 2.7 所示。

第 2 步：打开 Apocalypso 软件，准备对文件进行加密，如图 2.8 所示。

第 3 步：单击 Blowfish Encryption 按钮，进入到文件加、解密界面，如图 2.9 所示。

第 4 步：在 File to be Encrypter/Decrypted 文本框中选择要加密的文件“text.txt”，如图 2.10 所示。

第 5 步：在 Output File 文本框中选择加密后的文件存放位置，并将加密后生成的文件取名为 text2.txt，如图 2.11 所示。

第 6 步：在 Enter Passphrase here 文本框中输入加、解密的密码“aa”，如图 2.12 所示；

然后单击 Encrypt File 按钮，文件开始加密，直到出现加密结束提示，如图 2.13 所示。

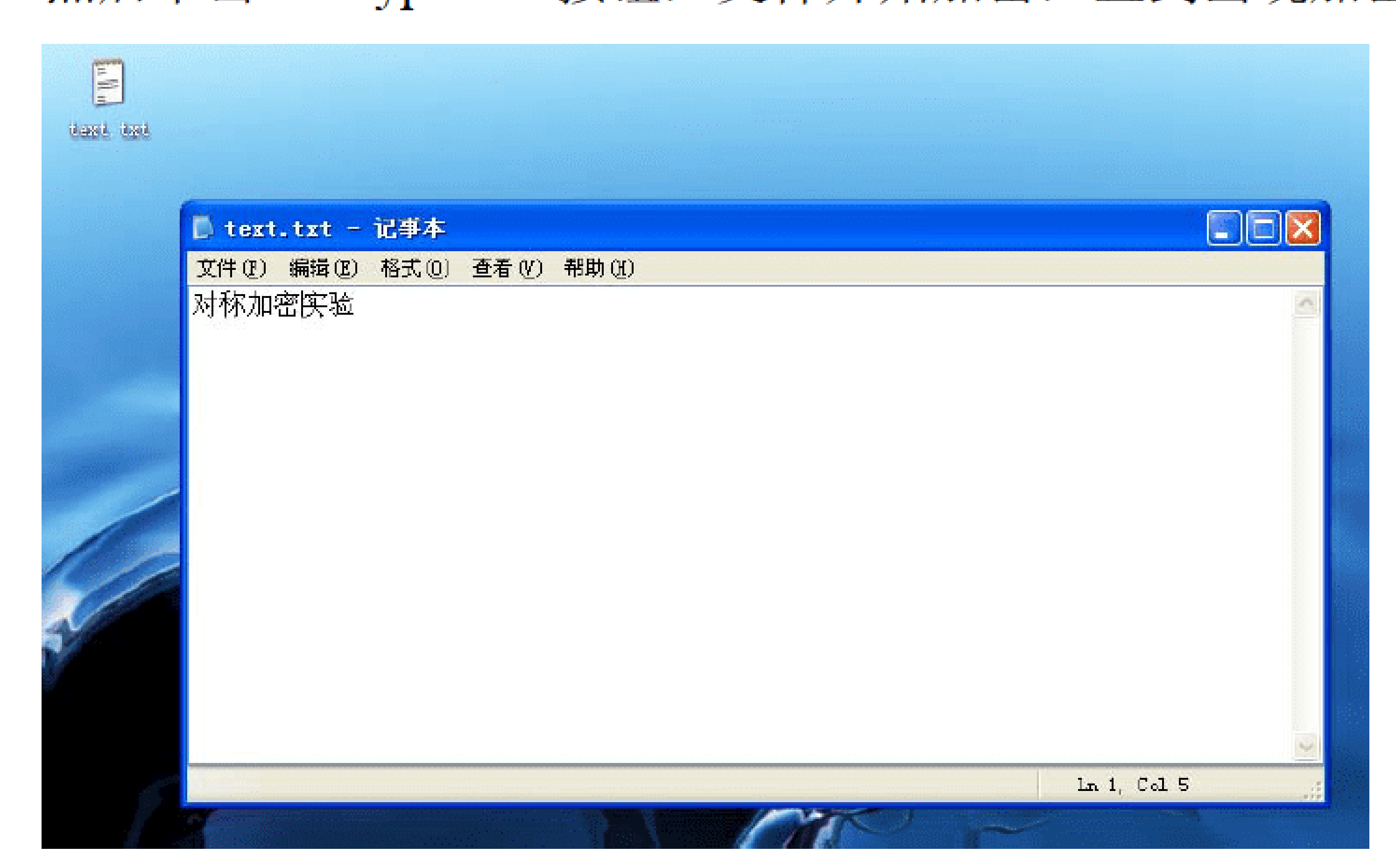


图 2.7　创建一个文本文件



图 2.8　打开“Apocalypso”软件主界面

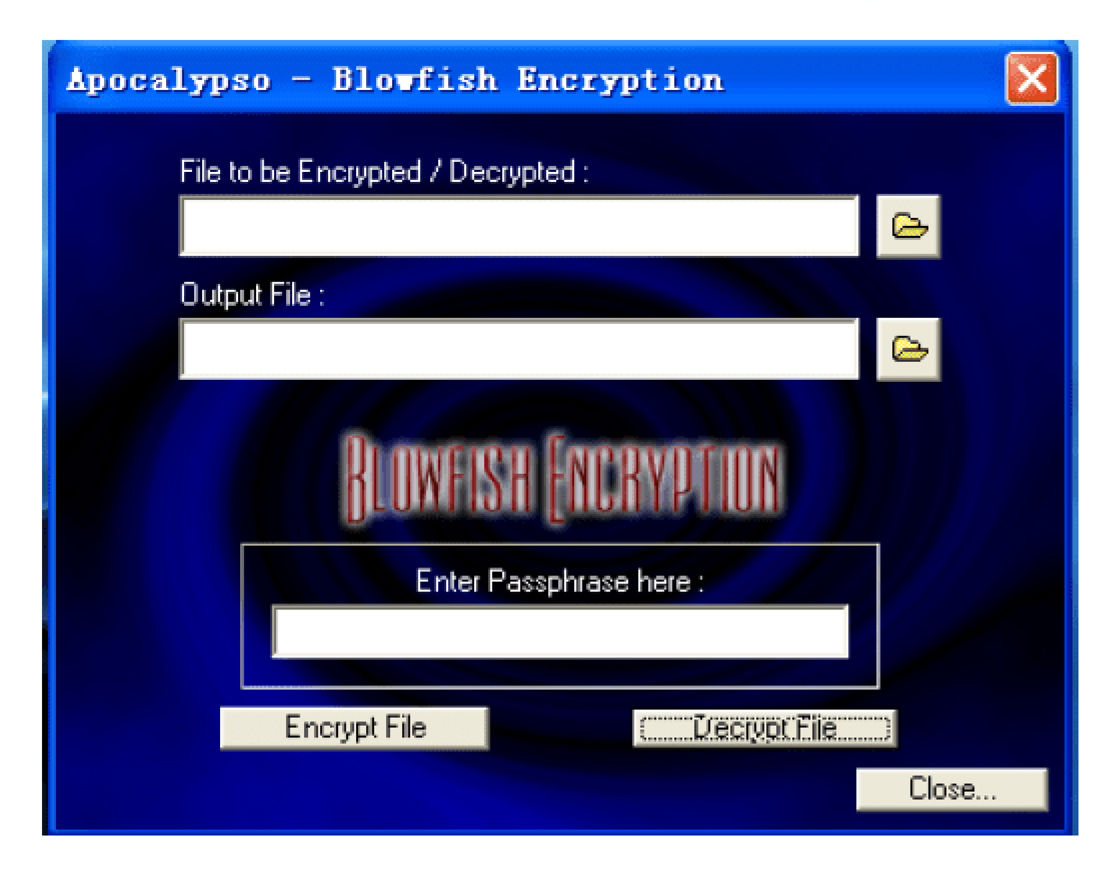


图 2.9　进入到文件加、解密界面



图 2.10　选择要加密的文件“text.txt”

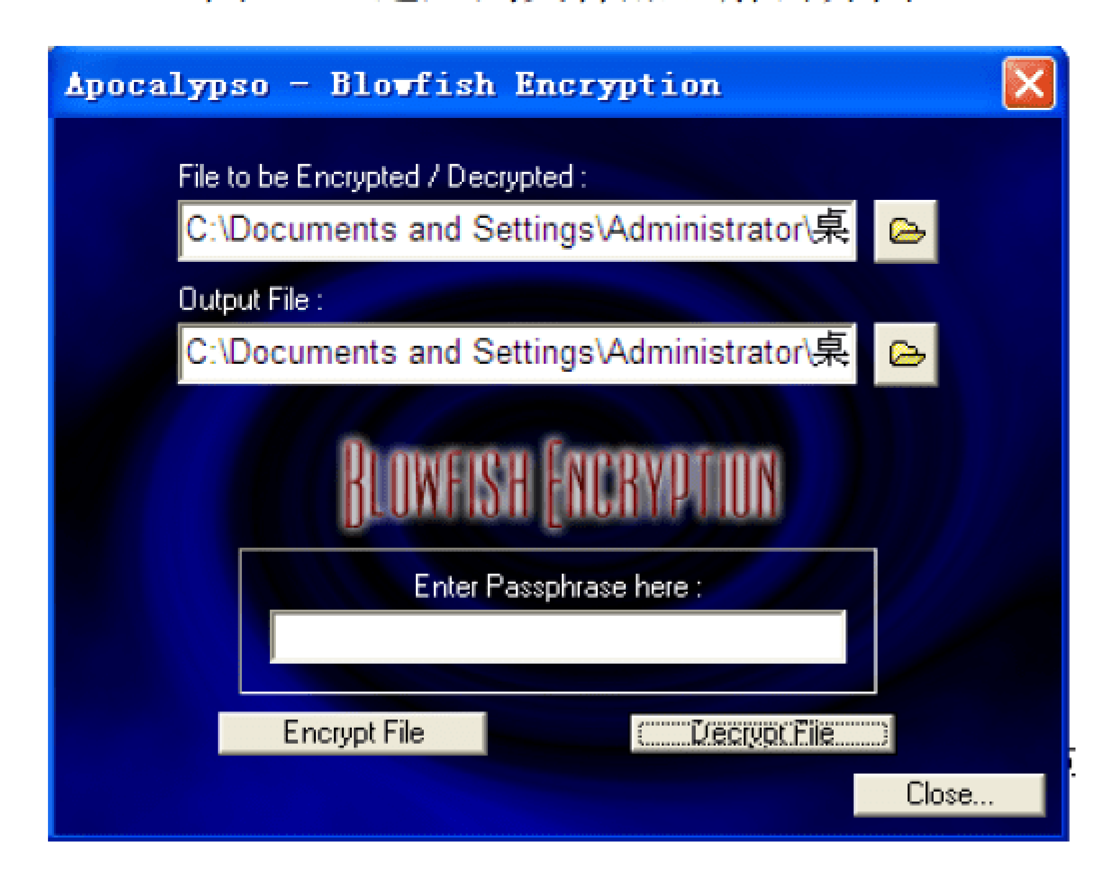


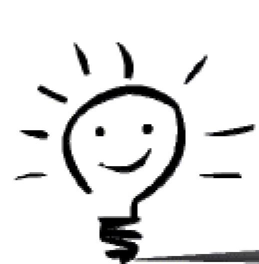
图 2.11　选择加密后的文件存放的位置



图 2.12　输入加、解密的密码

第 7 步：找到加密后文件“text2.txt”，双击打开，看到文档内容为乱码，说明已被加密，如图 2.14 所示。

第 8 步：解密。同样单击 Blowfish Encryption 按钮，进入到文件加、解密界面。在 File



to be Encrypter/Decrypted 文本框中选择要解密的文件“text2.txt”，在 Output File 文本框中选择解密后的文件存放位置，并将解密后生成的文件取名为 text3.txt。在 Enter Passphrase here 文本框中输入加、解密的密码“aa”，然后单击 Decrypt File 按钮，文件开始解密，如图 2.15 所示，直到出现解密结束提示，如图 2.16 所示。

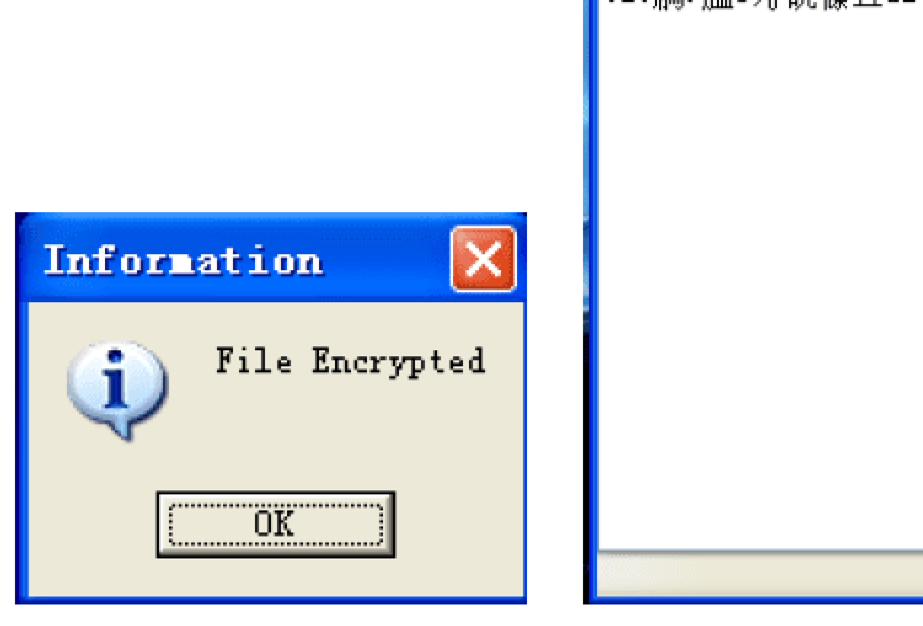


图 2.13 加密结束提示 图 2.14 加密后的文件“text2.txt”





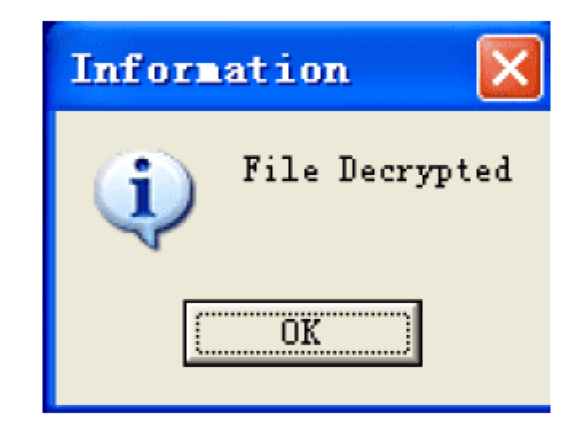


图 2.15 解密文件 图 2.16 解密结束提示

第 9 步：找到解密文件后的文件“text3.txt”，双击打开，原密文已恢复为明文，说明文件已被解密，如图 2.17 所示。

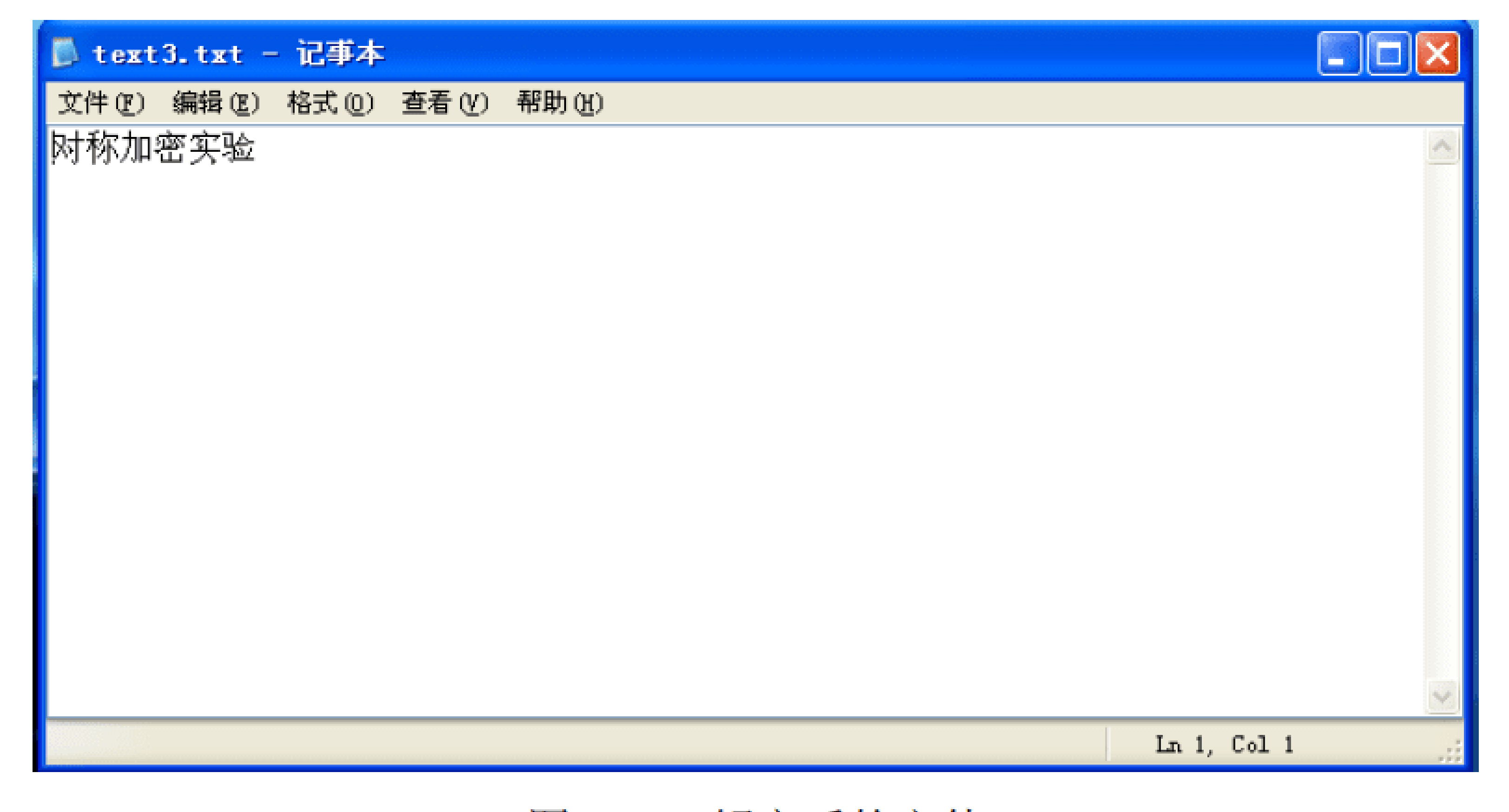


图 2.17 解密后的文件



实训 2　数据加密软件 PGP 的使用

实训目的

（1）掌握 PGP 软件的原理。
（2）掌握利用 PGP 软件加密数据的方法。

实训环境

（1）一台连上 Internet 的计算机。
（2）Windows XP/2000/2003 操作系统，PGP 软件。

操作步骤

1. 下载并安装 PGP 软件

PGP 是国外的一个免费英文软件，一般专业软件下载网站都提供下载。以 PGP 8.0.1 为例，经解压缩后，双击 PGP 8.0.1 安装文件，出现如图 2.18 所示的画面。

按照提示，依次单击 Next 按钮，即可安装成功。重新启动计算机后，可在屏幕上显示 PGP 活动栏。

如图 2.19 所示，PGP 活动栏上的按钮从左到右依次是 PGPkey（密钥管理）、Encrypt（加密）、Sign（数字签名）、Encrypt（加密与签名）、Dectypt/Verify（解密/验证）、Wipe（清除）、Freespace Wipe（自由空间清除）。



图 2.18　PGP 安装

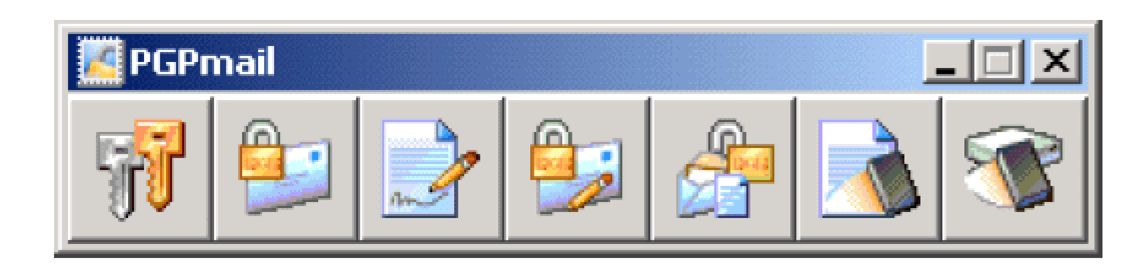


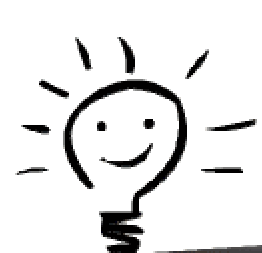
图 2.19　PGP 活动栏

2. 建立一对密钥的步骤

单击 PGPkey 按钮，然后依次完成以下操作：
（1）根据密钥生成向导，逐屏选择密钥的类型、密钥长度、密钥期限等。
（2）设置私钥传递词，以保护私钥。
（3）可以根据需要决定是否把密钥送到默认的服务器上。
（4）保存密钥。

3. 加密步骤

为了有一个实验对象，先在 C 盘下建立一个文件“PGPexecise.doc”。



（1）单击 Encrypt 按钮，在打开的 Select Files 对话框中选择用户将要进行加密的文件，选定后单击“打开”按钮。

（2）在 PGP key Selection Dialog 对话框中选择合作方的密码。

（3）输入自己的私钥，将 PGPexecise.doc 转换为.pgp 文件。

4. 解密步骤

（1）接收者输入自己的密钥，即可解密文件。

（2）在 PGPLog 对话框中查看文件的签名状态。

第 3 章
网络通信协议与安全

知识目标

- 了解 TCP/IP 协议以及工作原理。
- 了解以太网的工作原理。
- 理解使网络通信不安全的因素。
- 熟悉网络协议存在的安全问题。

技能目标

- 熟练应用常见的网络通信协议。
- 能够解决常见网络协议存在的安全问题。

计算机网络的基础是网络通信协议，保证通信协议的安全对计算机网络的安全有重要的意义。

3.1 TCP/IP 协议简介

TCP/IP 协议是先于 OSI 模型开发的，并不符合 OSI 标准。TCP/IP 模型是于 1974 年首先定义的，而设计标准的制定则在 20 世纪 80 年代后期完成。TCP/IP 实际上是由一组协议所组成，是当前 Internet 所使用的最流行的网络“标准”，虽然它不是国际标准，但由它所构成的系统经过不断地考验，日臻成熟，并且基于这个协议的网上应用广泛，所以这些年来，它已经成为事实上的国际标准。

构成 TCP/IP 的协议有很多。传输层的 TCP 协议、网际互联层的 IP 协议和许多别的协议共同构成了 TCP/IP 协议簇。其中最重要的两个核心协议是 TCP 协议与 IP 协议。

3.1.1 TCP/IP 协议以及工作原理

TCP/IP 协议由 TCP 协议和 IP 协议组成，它们是在 Internet 上的两个网络协议，分别叫做传输控制协议和互联网协议，属于众多 TCP/IP 协议簇中的一部分。

TCP/IP 协议簇中的协议保证了 Internet 上各种类型的计算机之间的数据传输，提供了几乎现在上网所用到包括电子邮件的传输、文件传输、BBS、新闻组的发布以及访问 WWW 的所有服务等。

1. TCP/IP 协议的四层模型

从协议分层模型方面来看，TCP/IP 由 4 个层次组成：网络接口层、网间网层、传输层和应用层，如图 3.1 所示。

HTTP SMTP INS FTP	SNMP RPC	应用层协议
TCP	UDP	传输层协议
IP ARP ICMP IGMP		网间网层协议
Ethernet	Token Ring	网络接口层

图 3.1　TCP/IP 协议的四层模型

（1）网络接口层。

网络接口层处于 TCP/IP 协议的最底层，负责接收 IP 数据报并通过网络发送，或者从网络上接收物理帧，抽出 IP 数据报，交给 IP 层。

（2）网间网层。

网间网层负责相邻计算机之间的通信，其功能包括：

① 处理来自传输层的分组发送请求。收到请求后，将分组装入 IP 数据报，填充报头，选择去往目标机的路径，然后将数据报发往适当的网络接口。

② 处理输入数据报。首先检查其合法性，然后进行寻址，假如该数据报已到达目标机，则去掉报头，将剩下部分交给适当的传输协议；假如该数据报尚未到达目标机，则转发该



数据报。

③ 处理路径、流量控制、拥塞等问题。

（3）传输层。

传输层提供应用程序间的通信。其功能主要是提供可靠传输。为实现后者，传输层协议规定接收端必须发回确认，假如分组丢失，必须重新发送。

（4）应用层。

应用层向用户提供一组常用的（如电子邮件、文件传输访问、远程登录等）应用程序。远程登录 Telnet 是使用 Telnet 协议提供在网络其他主机上注册的接口。Telnet 会话提供了远程的虚拟终端。文件传输访问 FTP 是使用 FTP 协议来提供网络内节点的文件复制功能。

2. TCP/IP 协议的工作原理

TCP/IP 通过协议栈工作，这个栈是所有用来在两台计算机间完成一个传输的所有协议的几个集合。这也就是一个通路，数据通过它从一台计算机到另一台计算机。数据在通过了如图 3.1 所示的各个层后，就从网络的一台计算机到了另一台计算机上。栈的每一层都能从相邻的层中接收或发送数据，每一层都与许多协议相联系。在栈的每一层，这些协议都在起作用。

3. IP 地址

Internet 上的计算机和网络设备很多，它们相互之间在进行信息交换时必须先给每台计算机或网络设备取一个名字，称为 Internet 地址，即 IP 地址，它是用来表明网络上的每一台计算机或网络设备自己身份的地址，并且是唯一的。在 Internet 中，IP 地址不是任意分配的，它必须由相应的组织进行分配，如中国教育科研网（CERNET）的用户必须向 CERNET 网络管理中心申请。TCP/IP 协议对这个地址做了规定，一个 IP 地址由一个 32 位二进制数表示，共分为 4 组，每 8 位为一组，每组数字的取值范围为 0～255，相互之间用圆点（.）分隔，表示形式为 XXX.XXX.XXX.XXX，如 192.168.0.100。一个 IP 地址由一个网络部分和一个主机部分组成，如图 3.2 所示。

网络地址部分	主机地址部分

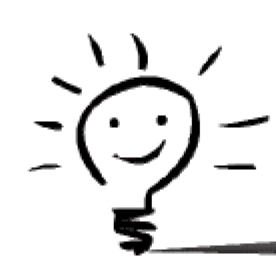
图 3.2　IP 地址的格式

为了有效地利用地址空间，根据选择的网络地址和主机地址位数的不同对 IP 地址分类，IP 地址分为 A、B、C、D 和 E 5 大类，最重要的是 A、B 和 C 类 IP 地址。

通过 IP 地址的前三位，就能区分出 IP 地址是属于 A 类、B 类或 C 类，如 IP 地址的最高位为 0，则是 A 类 IP 地址，第一字节的值为 0～127，A 类 IP 地址的主机容量为 16777216。B 类 IP 地址的最高两位为 10，第一字节的值为 128～191，B 类 IP 地址的主机容量为 65536。而 C 类 IP 地址的最高三位是 110，第一字节的值为 192～233，主机号只有 8 位，因此只能有 256 台主机。

将 IP 地址分成网络和主机部分，在路由寻址时非常有用，可以大大提高网络的速度。路由器（router）就是通过 IP 地址的网络号来决定是否发送和将一个数据包发送到什么地方。

一个网络设备可以有多个 IP 地址，比如连在两个物理网络上的路由器，它就有两个 IP



地址，分别连在两个不同的物理网络上，所以又可以将 IP 地址看成是一个网络连接。网络上的代理服务器也可能使用两块网卡，配置两个属于不同网络的 IP 地址，或使用一块网卡配置两个属于不同网络的 IP 地址（如 Windows NT 操作系统中），即一个外部网络地址，一个内部网络地址。

3.1.2 以太网

1. 以太网原理

局域网发展到今天，在实际应用中已相当普及。在各种局域网技术中，以太网被广泛使用。

以太网（Ethernet）是一种产生较早且使用相当广泛的局域网，其最早是由美国 Xerox（施乐）公司创建的，在 1980 年由 DEC、Intel 和 Xerox 3 家公司联合提出了以太网规范，这是世界上第一个局域网的技术标准。后来的以太网国际标准 IEEE802.3 就是参照以太网的技术标准建立的，两者基本兼容。为了与后来提出的快速以太网相区别，通常又将这种按 IEEE802.3 规范生产的以太网产品简称为以太网。

所有的以太网，不论其速度或帧类型是什么，几乎都遵从载波侦听多路访问/冲突检测（CSMA/CD）的通信规则。以太网的存取方式是一种采用随机访问技术的竞争型（有冲突）的访问方法。因为多台计算机可以同时使用以太网，每台计算机根据是否有载波信号出现来判定总线是否空闲。如果主机接口有数据要传输，它就侦听，看总线上是否有信号在传输。如果没有探测到，它就开始传输。每次传输都在一定的时间间隔内，即传输的数据包有固定的大小。而且硬件还必须在两次传输之间，观察一个最小的空闲时间，也就是说，总线上的计算机使用通信线路的通信机会是均等的。

当开始一个传输时，信号并不能同时到达网络的所有地方，这就有可能使两个设备同时探测到网络是空闲的，并都开始传输，当这两个信号在网络上相遇时，它们就都不再可用了，这种情况就叫做冲突（collision）。

以太网在处理这种情况时，很有技巧性。每台设备在它传输信号时都监听总线，看它传输时是否有信号干扰，这种监视叫做冲突侦听，在探测到冲突后，设备就停止传输。在以太网上，有可能会因为所有设备都忙于尝试传输数据而每次都产生冲突。

为了避免这种情况，以太网使用一个二进制后退策略。发送者在第一次冲突后，等待一个随机时间，再进行第二次传输，如果第二次还是冲突，则等待时间延长一倍，第三次再延长一倍，以此类推。通常这种策略，即使两台设备第二次等待的时间会很接近，但由于后面的等待时间成指数倍增长，不久，它们就不会冲突了。

2. 以太网的帧地址

每台连接到以太网上的计算机都有一个唯一的 48 位（二进制数）以太网地址。以太网卡厂商都从一个机构购得一段地址，在生产时，给每块网卡一个唯一地址。通常，这个地址是固化在网卡上的，称为网卡的物理地址（MAC 地址）。

当一个数据帧到达时，硬件会对这些数据进行过滤，根据帧结构中的目的地址，将属于发送到本设备的数据传输给操作系统，而忽略其他任何数据。



3.2　网络通信不安全的因素

生活中，经常会看到或听到这样的消息，一个黑客入侵了某一网络，使该网络的服务器全部瘫痪；一个黑客利用网络从某一银行盗取了大量钱财等。这些例子说明 Internet 是不安全的，Internet 需要更多、更好的安全机制。事实上，世界上没有绝对安全的网络，只要用户的计算机网络连接到 Internet 上，它就存在着危险。安全问题的一个主要方面就是使用的 TCP/IP 协议本身就存在着巨大的安全缺陷，包括建立在其上面的很多服务。

3.2.1　网络自身的安全缺陷

Internet 的基石是 TCP/IP 协议，该协议在实现上力求简单高效，而没有考虑安全因素。因为如果考虑安全因素，无疑会增大程序代码量，从而降低 TCP/IP 的运行效率，所以说 TCP/IP 协议本身在设计上就是不安全的，主要存在以下的安全缺陷。

1. 容易被窃听

大多数 Internet 上的数据信息流是没有加密的，电子邮件口令、文件传输等很容易被监听和劫获，可以实现这些行为的工具很多，还有很多免费提供此类工具的网站。

2. 脆弱的 TCP/IP 服务

在 Internet 上，很多基于 TCP/IP 协议的应用服务都在不同程度上存在着安全问题，这很容易被一些对 TCP/IP 协议十分了解的人所利用，尤其是一些新的处于测试阶段的服务有更多的安全缺陷。

3. TCP/IP 协议缺乏安全策略

由于技术水平原因，Internet 上的许多网络站点在防火墙的配置上无意识地扩大了访问权限，忽视了这些权限可能会被网络内部的人利用或滥用，黑客从一些服务中可以获得有用的信息，而网络管理或维护人员却不知道应该禁止这种服务。

4. 配置的复杂性

在 Internet 上，访问控制的配置一般是很复杂的，所以很容易被错误配置或配置不完善，使黑客有了可乘之机。

3.2.2　网络容易被窃听和欺骗

由于局域网的特点使得网络极易被窃听。Internet 是把无数的局域网连接起来形成一个大网，然后再把大的网连接成更大的网，从而形成一个庞大的网络。它的拓扑结构是一种逐步细化的树状结构，虽然 Internet 上的信息传输是点对点的，但一般 Internet 的主机会处于一个特定的局域网当中，例如一个学校的一个计算机实验室构成了一个局域网，它连接到学校的计算机校园网，校园网又连接到中国教育科研网（CERNET），CERNET 又连接到



了国内的其他网络或直接连到了国外的网络上。因为局域网（如以太网、令牌网等）都是广播型网络，也就是说，网络上的一台主机发布消息，网络上的任何一台机器都可以收到这个消息。一般情况下，以太网卡在收到发送给别人的消息时会自动丢弃消息，而不向上层传递消息。但如果我们把以太网卡的接收模式设置成混合型（promiscuous），这样网卡就会捕捉所有的数据包，并把这些数据包向上传递，这就造成了以太网可能被窃听。其实，光纤分布式数据接口（Fiber Distribrted-Data Interface，FDDI）、令牌网等也存在这样的问题。现在的 ATM 网络技术是点对点的，它不会像以太网的广播式网络那样容易被窃听。如图 3.3 所示为以太网卡混合工作方式和普通工作方式的工作原理。

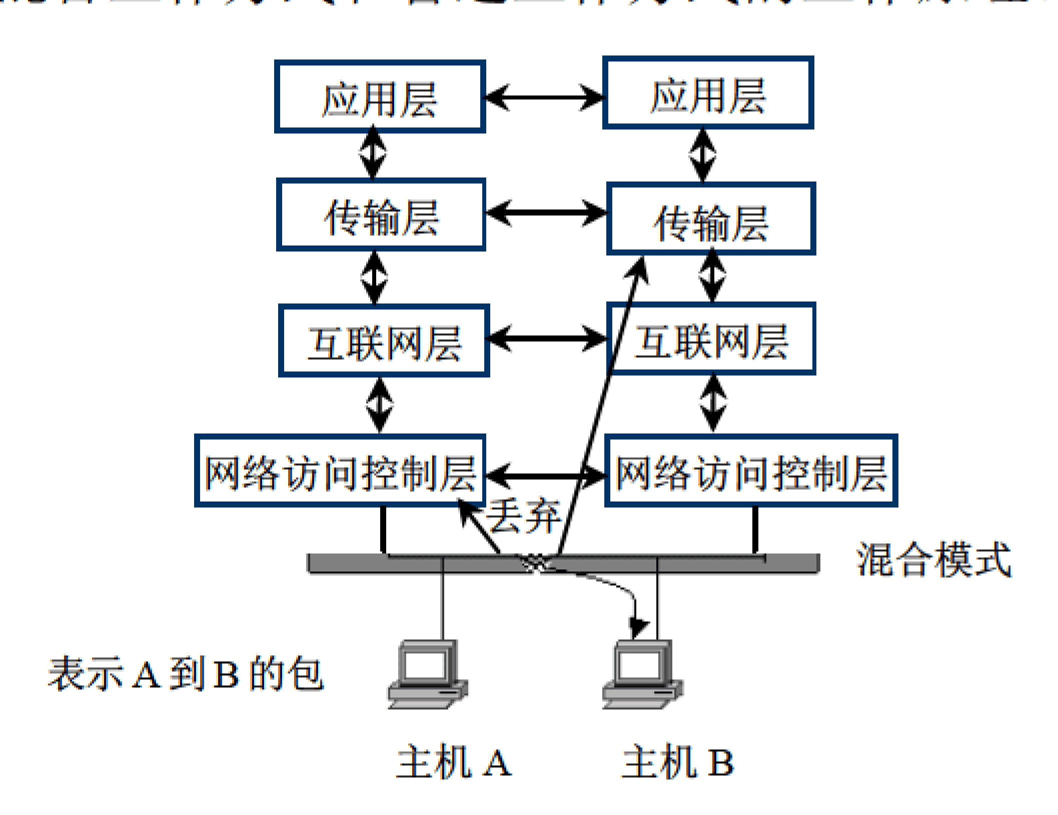


图 3.3　以太网卡混合工作方式和普通工作方式

Internet 上的信息，容易被窃听和劫获的另一个原因是，当有一个人用一台主机和网络上的另一台主机进行通信时，它们之间相互发送的数据信息包是经过很多机器（网络和路由器）重新转发的。如在公司计算机局域网内的一台主机上要访问 Hotmail 主机，用户数据包要经过公司局域网的路由器或代理服务器、公司网络的路由器、网络服务商的多个路由器，然后从总出口出去，再经过很多网络和路由器才能到达 Hotmail 主机。具体要经过多少主机、多少路由器和多少网络，不同的时候可能不同，用户可以用网络测试工具得到。如图 3.4 所示为网络上数据信息层层传递的工作原理。

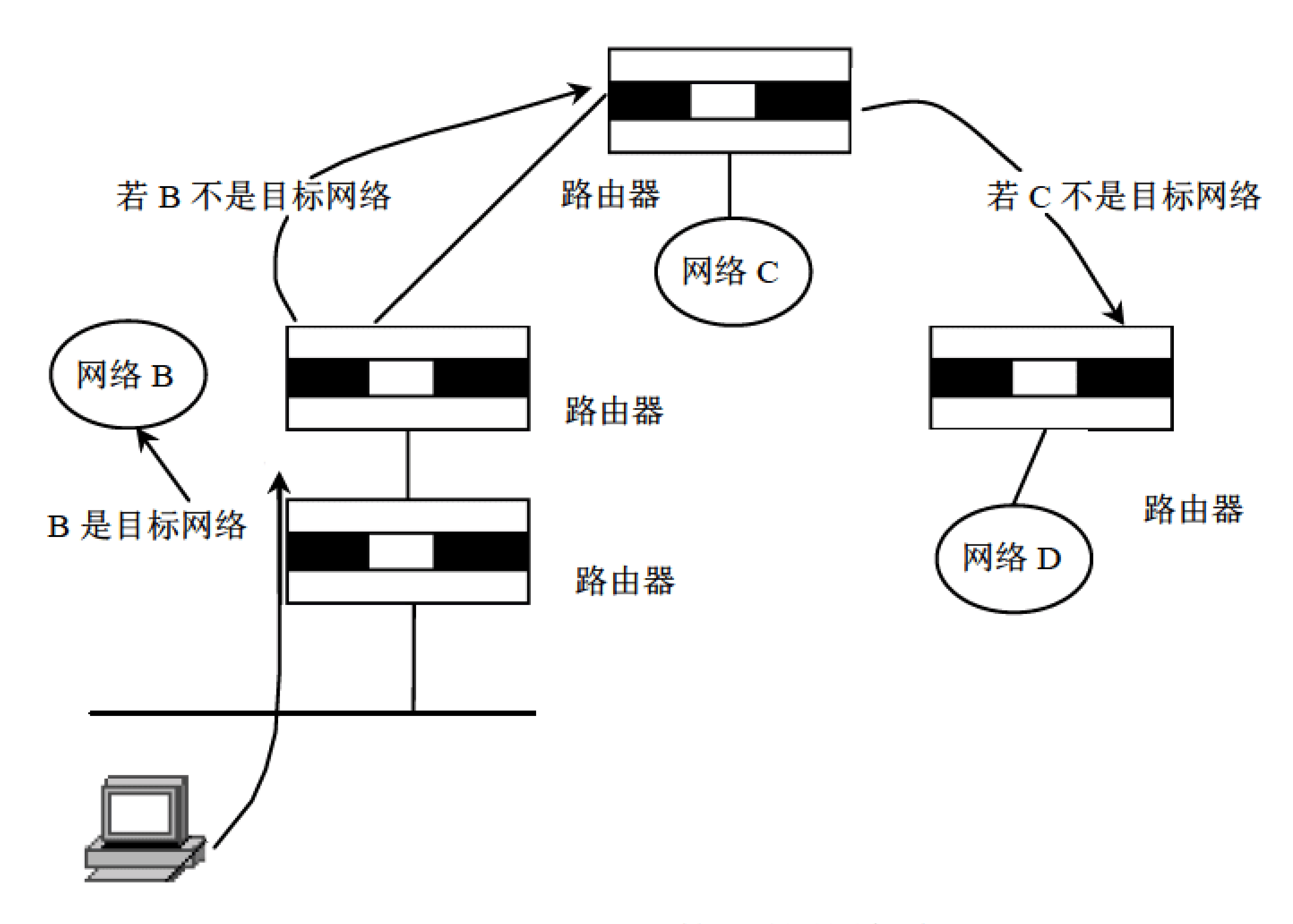


图 3.4　Internet 上数据的传输过程

因为 Internet 的这种工作原理不仅节约了资源，而且简化了传输过程的实现，符合 TCP/IP 协议简单、高效的宗旨，但这也带来了安全上的问题。当然用户不可能力求安全而放弃这种方法，因为这样做是不实际的，也是没有必要的。用户所能做的只是意识到这种问题，并以其他方法来解决这种问题，提高系统的安全性。在数据的传输过程中，如果一个黑客可以使用一台处于用户的数据包传输路径上的主机，那么他就可以窃听或劫持用户的数据包。例如，处于每个网络出口上的机器（比如网络上的边界路由器）就可以监听所有从这个网络进出的数据包，这和以前经过总机接转的电话监听是类似的。实际上，网络流量的统计和防火墙等都是利用了这个原理来实现的。网络上的窃听可能是出于好奇，也可能是恶意的。现在，越来越多的黑客不再是喜欢破坏公物的人，多数是出于商业目的，所以网络安全是把 Internet 真正推向商业化所必须要考虑和解决的问题。如图 3.5 所示为这种类型的窃听过程。

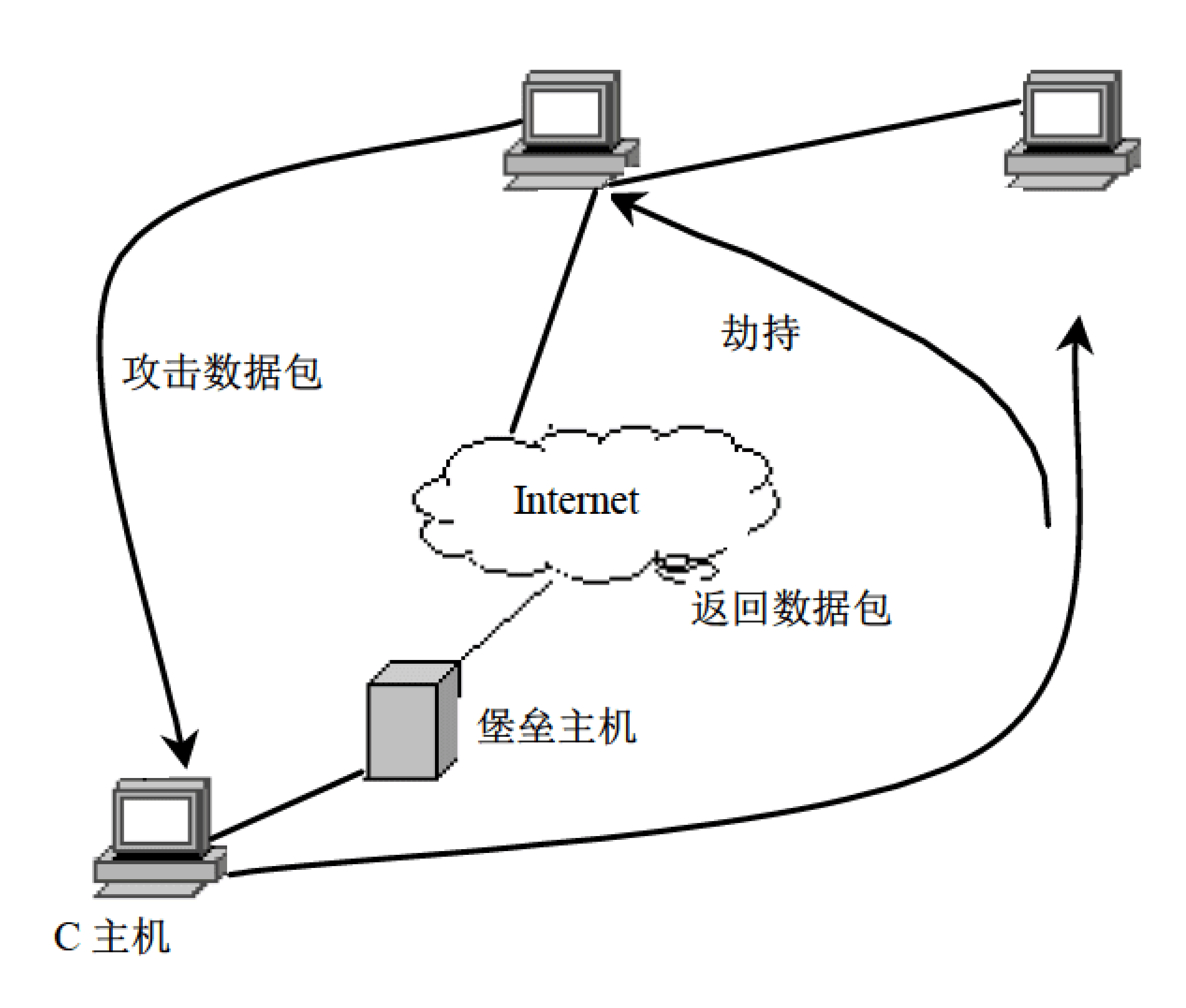


图 3.5　数据在传输过程中被窃听或劫持

电子欺骗（Spoofing Attack）是针对 HTTP、FTP 和 DNS 等协议的攻击，可以窃取普通用户甚至超级用户的权限，任意修改信息内容，造成巨大危害。常见的电子欺骗有 DNS（Domain Name Service）欺骗和 IP 地址欺骗两种。

电子欺骗的一种形式是 DNS 欺骗，它是利用了 DNS 服务本身的脆弱性。DNS 是其他 Internet 服务，如 WWW 服务、FTP 服务和电子邮件服务 SNMP 的基础，它负责把输入的域名转换成 IP 地址。

网络上的 DNS 服务器很多，这些服务器里有一个数据库，它记录着 IP 地址和域名的对应信息。当用户的主机向这些服务器查询转换信息时，这些主机就会回答用户的查询，从而得到要查找的主机的 IP 地址。DNS 欺骗的关键在于这些服务器不一定知道用户所要的信息，于是该服务器会向别的服务器查询，并且它对查询结果不加确认就放入自己的数据库中，并回答给用户。比如，在现实生活中有这样的例子，用户想知道 D 是不是一个可信任的人，于是去问 A，可是 A 不能回答这个问题，于是 A 去问 B，B 知道 D 是不



可信任的，于是告诉 A，然后由 A 再告诉用户。试想，D 为了不让用户知道他的真实面目，他会设法让他的好友告诉 A，D 是可信任的，而 A 又是一个不负责任的人，他不会去核实这个消息，于是当有用户再次去问 A 时，A 会告诉用户，D 是一个可以信任的人。这就是为什么会有 DNS 欺骗的原因。如图 3.6 所示为 DNS 欺骗的过程。

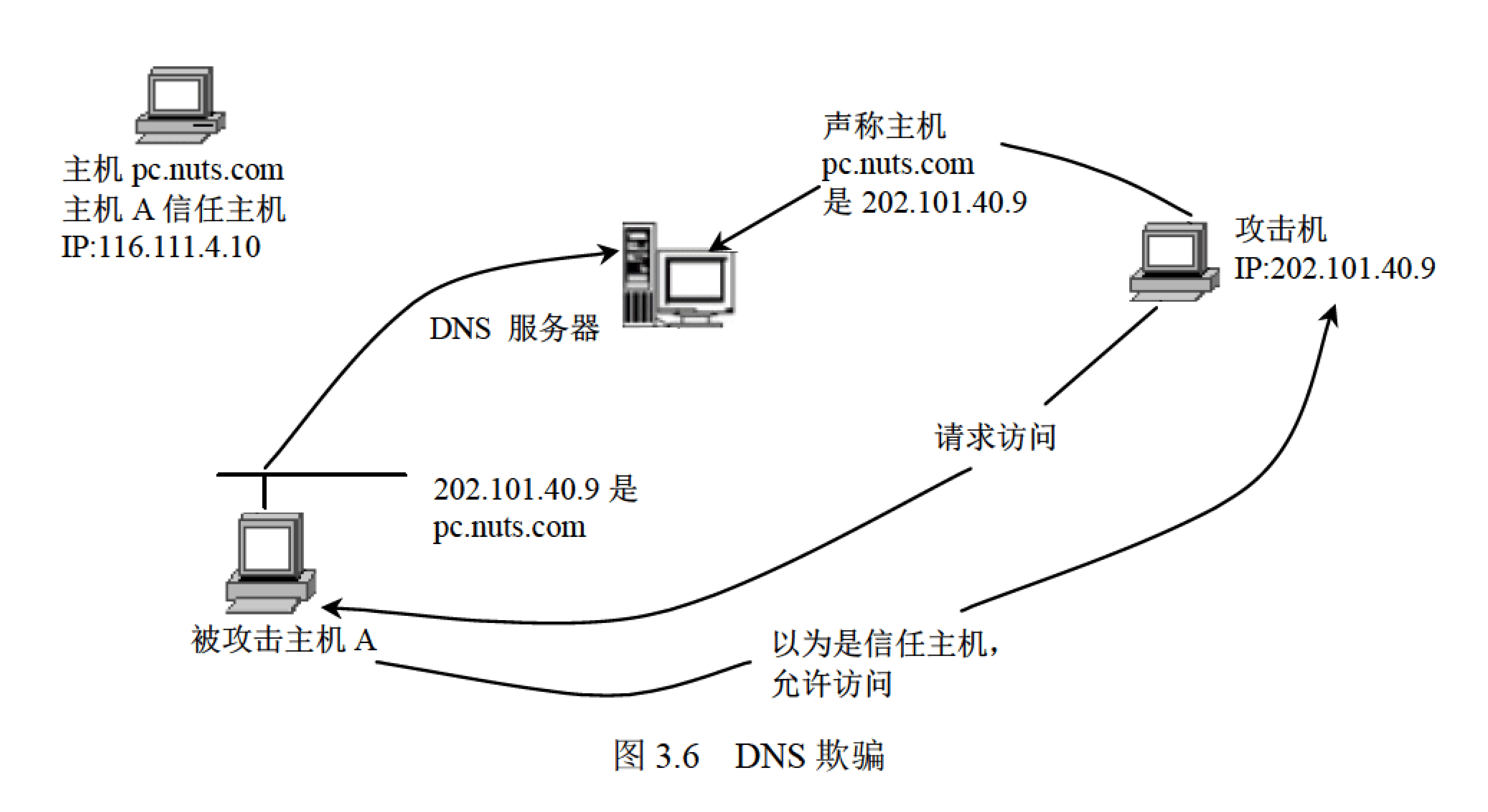


图 3.6　DNS 欺骗

IP 地址欺骗也是一种电子欺骗，就是伪造他人的源 IP 地址，其实质上就是让一台机器来扮演另一台机器，借以达到蒙混过关的目的。Internet 上的每一台主机都有一个 IP 地址，当用户的数据包将要离开主机网卡端口时，数据包上被自动加上主机的 IP 地址，这样接收者就知道是谁发来的数据信息。因为 TCP/IP 协议的实现代码是公开的，所以人们能很容易地开发出一种工具软件，让使用者指定数据包的源 IP 地址，实现 IP 地址的伪装，从而产生欺骗行为。下面一些服务相对来说容易招致此类攻击。

（1）任何使用 sunrpc 调用的配置。rpc 指 Sun 公司的远程过程调用标准，是一组工作于网络之上的处理系统调用的方法。

（2）任何利用 IP 地址认证的网络服务。

（3）X-Window 系统。

（4）各种 r 服务。在 UNIX 环境中，r 服务包括 rlogin 和 rsh，其中 r 表示远程。人们设计这两个应用程序的初衷是向用户提供远程访问 Internet 网络上主机的服务。r 服务极易受到 IP 欺骗的攻击。

请看一个例子，假如黑客主机攻击 A 主机，并且打算伪装成 B 主机和 A 进行会话，黑客的主机为 C 主机。黑客从 C 主机发出 TCP 连接请求，但使用了 B 主机的 IP 地址，A 主机在收到请求数据包后，向 B 主机发出应答数据包。黑客不会让 B 主机收到 A 主机发出的应答数据包，因为那样 A 主机会知道有人在冒充 B 主机。使 B 主机不能接收到 A 主机发出的应答数据包的方法有 3 种，第一种是劫持 A 主机发出的数据包，第二种是用大量的连接请求数据包淹没 B 主机，使它无机会处理来自 A 主机的数据包，第三种是改变主机 A 到



主机 B 的路由，使数据包不能到达 B 主机，于是黑客就可以在 A 主机不察觉的情况下冒充 B 主机进行对话了。如图 3.7 所示描述了这个过程。

几乎所有的电子欺骗都依赖于目标网络的信任关系，解决电子欺骗的途径是慎重设置和处理网络中的主机信任关系，尤其是不同网络之间主机的信任关系。如只存在局域网内的信任关系，可以设置路由器使之过滤掉外部网络中自称源地址为内部网络地址的 IP 数据包，从而抵御 IP 欺骗。目前，Cisco System 和 ISS 等公司提供了一些安全软件包，其具有测试网络在 IP 欺骗上的漏洞的功能。

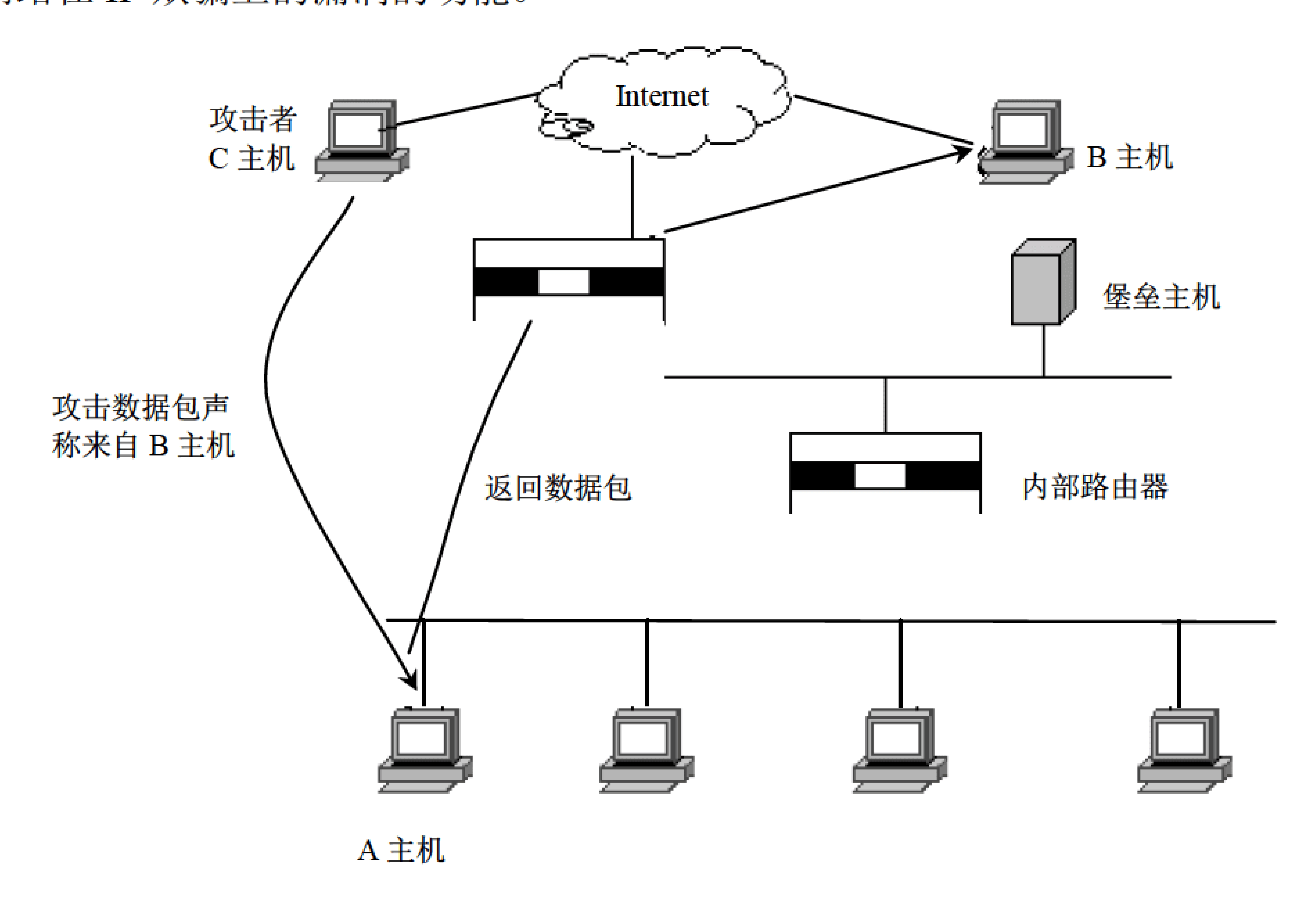


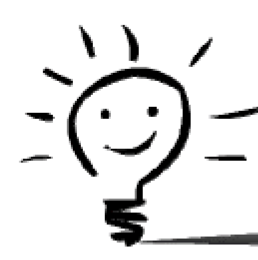
图 3.7　IP 地址欺骗

3.2.3　脆弱的 TCP/IP 服务

基于 TCP/IP 协议的 Internet 服务很多，包括 WWW 服务、电子邮件服务、FTP 服务、TFTP 服务、NFS 服务和 Finger 服务等。这些服务都存在不同程度的安全缺陷。当用户用防火墙保护站点时，就应该清楚提供哪些服务、禁止哪些服务。

1.　电子邮件服务

电子邮件服务给人们提供了一种便宜、方便和快捷的服务，E-mail 甚至开始出现在人们的名片上，成为了最受欢迎的通信方式之一。现在，UNIX 操作系统环境下的电子邮件服务器一般是用 Sendmail，它是一个复杂且功能强大的应用软件，正因为如此，它的安全漏洞就更多。一般来说，程序越庞大、越复杂，出现安全漏洞的可能性就越大。Sendmail 在 UNIX 操作系统环境下以 root 账号运行，所以如果该程序被黑客利用，用户主机的损失将是十分巨大的。Internet 上的蠕虫病毒曾经震惊世界，它使大批的网络服务器陷于瘫痪之中，这种病毒就是利用了 Sendmail 的安全缺陷。如果使这些功能以更安全的方式实现，则



需要对 Sendmail 进行重新设计和重新实现，但人们又会担心新的版本会出现更多的人们不知道的安全漏洞。Sendmail 的安全问题被人们修修补补，但总是有新的问题出现。

除此之外，电子邮件的附件中的 Word 文件或其他文件中也可能会带有病毒，给系统安全带来麻烦。电子邮件炸弹就是一个令人头疼的问题。

2. FTP 服务

FTP 服务是用于传输文件的，可以用来下载任何类型的文件。网络上有许多的匿名 FTP 服务站点，其上有许多免费软件、图片和游戏等，匿名 FTP 是人们常使用的一种服务方式。匿名 FTP 服务就像匿名 WWW 服务一样是不需要口令的，但用户的权力会受到严格的限制。匿名 FTP 存在一定的安全隐患，因为有些匿名 FTP 站点提供了可写空间给用户，这样用户就可以上传一些软件到站点上浪费该站点磁盘空间、网络带宽等系统资源，还可能会造成“拒绝服务”攻击。匿名 FTP 服务的安全很大程度上取决于一个系统管理员的水平，一个低水平的系统管理员很可能会错误授权配置，从而被黑客加以利用，并破坏整个系统。

3. Finger 服务

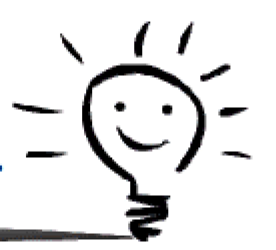
Finger 服务用于查询用户的信息，包括网上成员的真实姓名、用户名、最近的登录时间和地点等，也可以用来显示当前登录在机器上的所有用户名。这对于入侵者来说是无价之宝，因为它能告诉入侵者在本机器上有效的登录名，然后入侵就可以注意其活动了，等待时机成熟时再实施攻击。

4. 其他安全性极差的服务

除了上面提到的服务外，还有如 WWW、X-Window 系统服务、基于 RPC 的 NFS 服务和 BSD UNIX 系统的“r”开头的服务，如 rlogin、rsh 和 rexec 等。这些服务在设计上安全性极差，一般只在内部使用。如果网络有防火墙，就应该把这些服务限制在内部网络中。

3.2.4 缺乏安全策略

制定一个完善和成功的网络安全策略并不是一件容易的事情，需要网络使用者的通力合作，尤其需要管理部门的大力支持和配合。一般来说，单位管理部门制定网络的总体安全策略，系统管理员提供技术咨询和支持。很多企业或事业单位都建立了自己的内部局域网络（Intranet），并且通过不同的途径接入了 Internet。大多数人认为只要网络有防火墙，就能够保证网络的安全，但实际上防火墙战略只是网络总体安全策略中的一部分。例如，一个企业网络的网络管理员是一个网络安全专家，网络的防火墙上也无任何安全漏洞，但网络安全意识淡薄的职员可能会抱怨防火墙限制太多，而用拨号方式连接 Internet，这无疑给了黑客可乘之机，因为他可以通过电话线路绕过坚固的防火墙而进入用户网络内部。有些黑客实施社会工程攻击，攻击对象就是那些没有安全意识的职员，他会欺骗这些职员，让职员告诉他机器的口令等秘密数据信息。所以，人是安全策略的中心和重心，防火墙只是一种工具，安全策略实施得好与坏取决于人员的素质，对职员的安全意识教育和定期培



训是一种好的办法。

除了人为的因素外，另一个因素也妨碍着安全策略的执行，那就是系统和防火墙本身配置的复杂性。这对管理员要求很高。低水平的系统管理员常常会把防火墙配置错，这样就在防火墙上打开了安全漏洞。另外，防火墙的管理不仅仅是单击鼠标就可以的，系统日志的查看也是十分重要的，在日志文件中可以发现入侵的迹象，及时对防火墙的配置进行修改，防止入侵的扩展。当然，随着防火墙技术的发展，防火墙的配置也会像操作 Windows 那样简单，这样会推动防火墙的使用，更好地发挥防火墙的作用。

总之，一个好的安全策略的实施效果取决于职员的安全意识和网络管理者，尤其是网络安全管理员的计算机知识水平和技术能力。

3.2.5　来自 Internet 的威胁

Internet 上存在人为的威胁和自然的破坏。在这两个因素中，人为的破坏是更重要的，自然的破坏可以通过数据备份和冗余设置等来预防，人为的破坏则防不胜防。人为的破坏主要来自网络黑客，研究计算机网络犯罪现在已经成为犯罪学研究领域的一个重要部分，这些罪犯知识水平高、危害性大，而且隐蔽性很强，是一种高科技手段的犯罪行为。目前，在 Internet 上实行商业信息盗窃、银行抢劫等犯罪活动越来越多，网络黑客不仅是一些想显示自己计算机水平和计算机应用能力的好奇的大学生，更多的是一些专职的商业间谍，有的是对钱财的贪婪，有的是出于其他目的。另一种人为的破坏是来自网络内部，这种危害来自那些对企业或单位不满，或者是被解雇了的职员对内部网络的入侵，因为这种人对内部网络很了解，他们的这种入侵危害性很大。因此，网络管理人员及时地删除离职人员的账户是非常重要的。

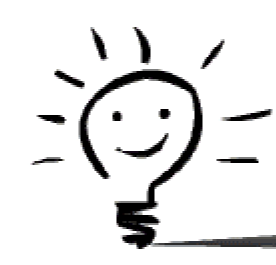
除了直接的网络入侵外，各种病毒程序也是 Internet 上潜在的巨大的危险，这些病毒可以在网络上随意传播，也可以通过下载的软件，如 Java 程序、ActiveX 控件等进入到内部网络，从而对网络造成危害。特洛伊木马就是一种病毒程序，它在表面上看起来是无害的，具有很强的隐蔽性，但它实际上却在背后破坏用户的网络。

虽然现在的防火墙都声称具有防病毒的功能，但新的病毒、旧病毒的变异品种是不会被发现的，它仍然会进入用户的网络，给网络造成危害。

3.3　网络协议存在的不安全性

网络层的协议是一些传输透明化的协议，如果不使用一些监视系统进程的工具，用户是看不见这些协议的。

Sniffers 是一种能看到这些步骤的装置，这个装置可以是软件，也可以是硬件，它能读取通过网络发送的每一个数据包，能读取发生在网络层协议的任何活动。它广泛地用于隔离用户看不到的、网络性能下降的问题，它会对网络的安全问题造成威胁。



网络层协议包括地址解析协议、Internet 控制消息协议、Internet 协议、传输控制协议等。

3.3.1 IP 协议与路由

1. IP 协议

IP 协议定义了一种高效、不可靠和无连接的传输方式。由于传输没有得到确认，所以是不可靠的。一个数据包可能丢失了，或看不见了，或是延时了，或是传输顺序错了，但是传输设备并不能检测到这些情况，也不通知通信双方。无连接则是因为每个数据包的传递与别的数据包是相互独立的，同一个计算机上的数据包可以通过不同的路径到达另一台计算机，或在别的计算机上已经丢失。由于传输设备都试图以最快的速度传输，所以是最高效的。

IP 协议定义了通过 TCP/IP 网络传输的数据格式和数据进行传递的路由功能。IP 数据包由头部分和数据部分组成，头部分包含诸如目的地址、源地址和数据的类型等信息。

2. IP 路由

在一个网络上，连接着两种基本设备：主机和路由器。路由器通常连接几个物理网络。对一台主机来讲，要将一个数据包发送到别的网络，就需要知道这个数据包应该走什么路径才能达到目的地。对一台路由器来讲，必须清楚将收到的数据包发往哪个物理网络。因此，无论主机还是路由器，在发送数据包时都要做路由选择。

数据发送有直接数据发送和间接数据发送两种方式。直接数据发送通常是在同一个物理网络里进行的。当一个主机或路由器要将数据包发送到同一物理网络上的主机时，就是采用这种方式的。首先判断 IP 数据包中的目的地址中的网络部分，如果是在同一个网络上，则通过地址分析，将 IP 数据包的目的地址转换成物理地址，并将数据包解开和该地址合成一个物理传输帧，通过局域网将数据包发出。间接数据发送是在不同物理网络之间进行的。当一个主机或路由器要将数据包发送到不同的物理网络上的主机时，这台设备就先在路由表中查找路由，然后将数据包发往路由中指定的下一个路由器，这样一直向外传送数据包，最后肯定有一个路由器发现数据包要发往同一个物理网络，于是，再用直接数据发送方式，将数据包发送到目的主机上。

主机和路由器在决定数据怎样发送时，都要去查找路由。一般都将路由组成一个路由表存放在计算机中。路由表一般采用（N，R）对表示，N 是目的地址的网络地址，R 是传输路径中的下一个路由。通常这个路由和这台计算机在同一个物理网络里。

3.3.2 TCP 协议

TCP 协议在 IP 协议之上，为其上的应用层提供了一种可靠的传输服务，这种服务的特点是可靠、全双工、流式和无结构传输。

TCP 协议使用积极确认和重发送技术来实现可靠传输。接收者在收到发送者发送的数据后，必须发一个相应的确认（ACK）消息，表示它已经收到了数据。发送者保存发送的



数据记录，在发送下一个数据前，等待这个数据的确认消息。在它发送这个数据的同时，还启动一个计时器，如果在一定的时间内，没有接收到确认消息，就认为是这个数据在传送时丢失了，接着就会重新发送这个数据。

这种方法产生了一个问题，就是数据包的重复。如果网络传输速度比较慢，等到等待时间结束后，确认消息才返回到发送者，那么由于发送者采用的是重复发送方法，就会出现重复的数据包。解决办法是给每个数据包分配一个序列号，并需要发送者记住哪个序列号的数据包已经确认了。为了防止由于延时或重复确认，规定确认消息里也要包含确认序列号，从而发送者就能知道哪个数据包已经确认了。

使用 TCP 传输就是建立一个连接，在 TCP 传输中一个连接由两个端点组成。其实一个连接代表的是发送者和接收者两端应用程序之间的一个通信，可以把它们想象成建立了一个电路，通常一个连接用（Host，Port）表达，其中，Host 是主机，Port 是端口。TCP 端口能被几个应用程序共享。对于程序员来讲，可以理解为一个程序可以为不同的连接服务。

TCP 传输数据的单位是段，在建立连接、发送数据、确认消息和告知窗口大小时均要进行段的交换。段的格式也分成头和数据两个部分。

TCP 协议使用三次握手来建立一个 TCP 连接。握手过程的第一个段的代码位设置为 SYN，序列号为 x，表示开始第一次握手，接收方收到这个段后，向发送者回发一个段，代码位设置为 SYN 和 ACK，序列号设置为 y，确认序列号设置为 x+1。发送者收到这个段后，就知道可以进行 TCP 数据发送了，于是它又向接收者发送一个 ACK 段，表示双方的连接已经建立。在完成握手后，就开始正式的数据传输了。

TCP 协议的这种属性，决定了它难以避免的安全隐患，目前在 Internet 上的安全问题中，很多攻击方式都是建立在 TCP 欺骗的基础之上的。

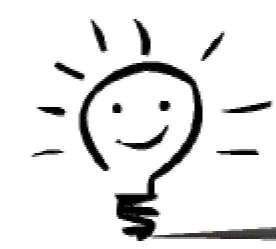
3.3.3　Telnet 协议

Telnet 协议的目的就是提供一个相当通用的、双向的、面向 8 位字节的通信机制。它的最初目的是允许在终端和面向终端的进程之间进行交互。Telnet 不仅允许用户登录到一个远程主机上，它还允许用户在那台计算机上执行命令。这样，用户在自己的局域网里的任何一台计算机上就可以 Telnet 到清华大学计算机校园网络上的一台计算机，并在这台计算机上运行程序。Telnet 没有图形功能，它仅提供基于字符界面的访问。

即使 GUI 应用程序被广泛采用，Telnet 这个建立在字符基础上的应用程序，仍相当地流行。其原因是：

（1）Telnet 允许用户以很小的网络资源花费实现各种功能（如收发电子邮件）。

（2）实现安全的 Telnet 是件十分简单的事，有许多这样的程序，通用的是 Secure Shell。要使用 Telnet，用户必须指定启动 Telnet 客户的命令，并在后面指定目标主机的名字。在 Linux 中，可以表示为“$telnet sctc.edu.cn”，这个命令启动 Telnet，连接到 sctc.edu.cn 网络的一个服务器上。这个连接可能被接受，或被拒绝，这与目标主机的配置有关。



Telnet 并不是一种非常安全的服务，虽然登录时它要求用户认证。由于 Telnet 发送的信息都未加密，所以信息容易被网络监听。仅当远程计算机及其与本地站点之间的网络通信安全时，Telnet 才是安全的。这就意味着在 Internet 上 Telnet 是不安全的。

除了 Telnet 外，还有几种程序能用于远程终端访问和执行程序，如 rlogin、rsh 和 on。在受托的环境里使用这些程序，允许用户远程登录而无须重新输入口令。他们登录的主机相信用户所用的主机已对其用户做过认证。但是使用这几个 r 命令是特别不安全的，容易受到 IP 欺骗和名字欺骗以及其他的欺骗技术的攻击，因此，托管主机模式并不适合在 Internet 上使用。

在设有防火墙保护的网络内使用 rlogin 和 rsh 是可以的，这取决于企业内部的安全措施。然而，on 依靠客户机程序进行安全检查，每个人都可以假冒客户机而回避检查。因此，on 是很不安全的，即使在设有防火墙的局域网内使用也是如此，因此最好使 on 命令失效。

3.3.4 文件传输协议 FTP

文件传输协议 FTP 是从一个系统向另一个系统传递文件的标准方法。它的目标是：

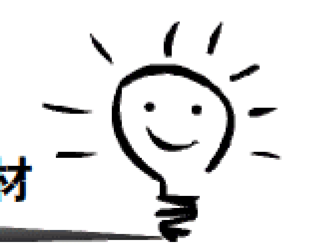
- ☑ 促进文件和程序的共享。
- ☑ 鼓励间接和含蓄地使用远程计算机。
- ☑ 使用户不必面对主机间使用的不同的文件存储系统。
- ☑ 有效和可靠地传输文件。

FTP 应用在 C/S（Client/Server）环境。请求计算机启动一个 FTP 客户端软件，这就给目标文件服务器发出了一个请求。典型的是，这个要求被送到端口 21。一个连接建立起来后，目标文件服务器必须运行一个 FTP 服务软件。

大多数站点担心的是用户会带入有破坏性的软件以及一些计算机游戏、盗版软件和黄色图片，这些东西花费大量的时间并占用磁盘空间，但这并不是主要的安全危险。在进行 FTP 传输时应当注意，千万不要轻信通过 FTP 传来的任何软件。

对于使用匿名 FTP 服务，用户可以用“匿名”用户名登录 FTP 服务器。通常情况下，这要求用户提供完整的 E-mail 地址作为响应。然而在大多数站点上，这个要求不是强制性的，只要它看起来像 E-mail 地址（比如是否包含@符号），它不对口令做任何方式的校验。要确保匿名 FTP 服务器只能存取允许存取的信息，不允许外人存取本机的其他资料，如私人资料等。在 FTP 服务器处理匿名用户命令前，许多 FTP 服务器执行 chroot 命令进入匿名 FTP 区。然而为了支持匿名 FTP 和用户 FTP，FTP 服务器要访问所有文件，这就是说 FTP 服务器总是在 chroot 环境中运行。

为了解决这个问题，可以通过修改系统的配置来代替直接启动 FTP 服务器，它执行 chroot，然后再启动 FTP 服务器。建立匿名 FTP 系统的具体技术依赖于操作系统使用的特定 FTP 管理程序（守护程序）。



匿名用户获取到的不应见到的文件，通常是由于内部客户将文件放在匿名 FTP 区而实现的。如果不希望外界阅读自己的文件，最好不要给匿名的 FTP 提供文件。匿名 FTP 区的可写路径无论使用何种 FTP 守护程序，都将面临一个特殊的问题：匿名 FTP 区的可写性。站点经常为此区提供空间，以便外部用户能用它上传文件。

可写区是非常重要的，但也有不安全的因素。因为这样的可写路径一旦被发现，就会被 Internet 上的“地下用户”用做“仓库”和非法资料的集散地。

本 章 小 结

计算机网络的基础是网络通信协议，保证通信协议的安全对计算机网络的安全有重要的意义。

TCP/IP 协议本身在设计上就是不安全的，主要存在以下的安全缺陷：网络容易被窃听和欺骗；TCP/IP 服务的脆弱性；缺乏安全策略；配置的复杂性。

习　　题

一、填空题

1．TCP/IP 模型 TCP/IP 协议簇中最重要的两个核心协议是__________协议与____________协议。

2．说 TCP/IP 协议本身在设计上就是不安全的，主要存在___________、___________、_________、_________的安全缺陷。

3．电子欺骗是针对_________等协议的攻击。

4．IP 欺骗，就是伪造他人的_________。

5．基于 TCP/IP 协议的 Internet 服务有__________、_________、_________、_________、_________等。

二、简答题

1．什么是 TCP/IP 协议？试述它的工作原理。

2．TCP/IP 协议存在哪些安全问题？

3．网络本身存在哪些安全问题？

4．网络为什么是不安全的？

5．Internet 上存在哪些威胁？

6．什么是电子欺骗？电子欺骗有哪些形式？

7．FTP 存在哪些安全隐患？如何解决？



本 章 实 训

实训 Telnet 漏洞攻击与防范

实训目的

（1）了解计算机通信协议漏洞的常见形式。

（2）掌握 Telnet 漏洞攻击与防范方法。

实训环境

（1）局域网主机。

（2）Windows NT/2000/2003 系统。

操作步骤

第 1 步：建立 IPC$连接（假设使用 X-scan 扫描器扫描到目标主机账号为“administrator”，密码为空），如图 3.8 所示。

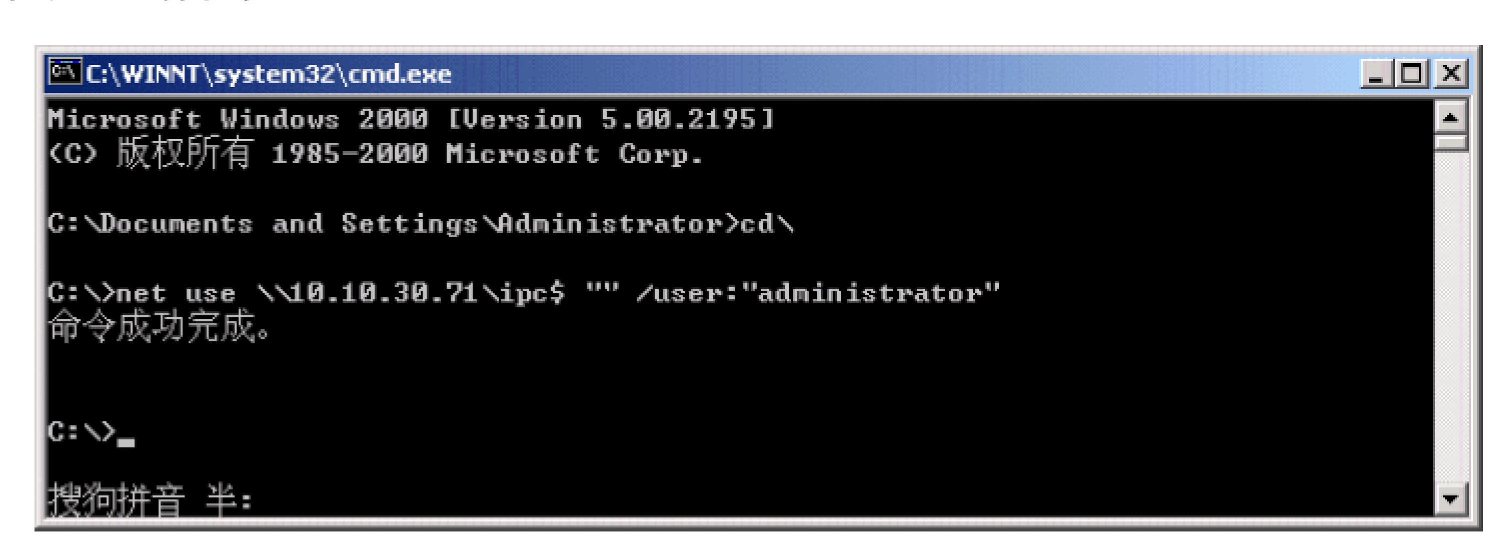


图 3.8 建立 IPC$连接

第 2 步：开启远程主机中被禁用的 Telnet 服务，如图 3.9 所示。

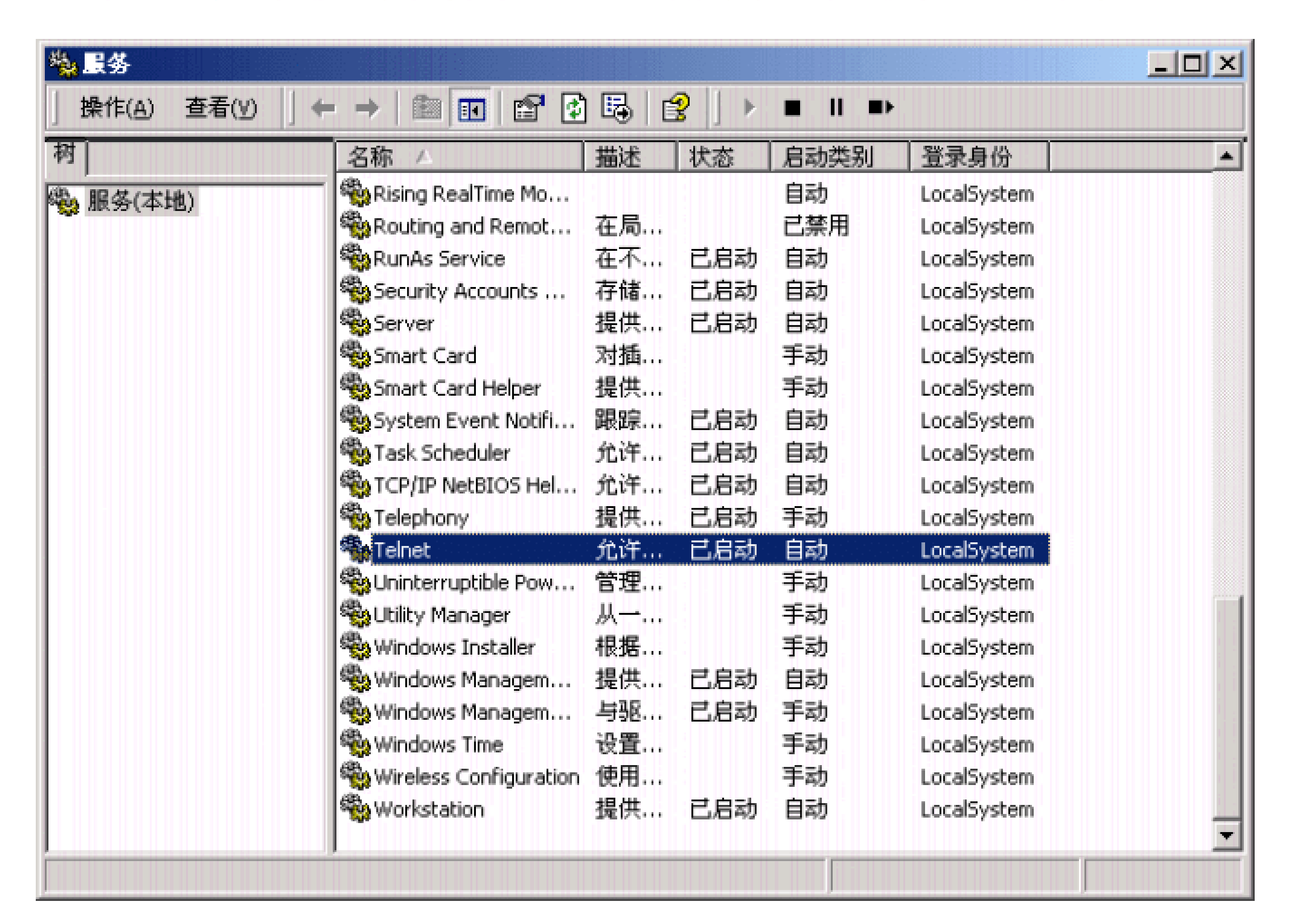


图 3.9 开启远程主机中被禁用的 Telnet 服务



第 3 步：断开 IPC$连接，如图 3.10 所示。

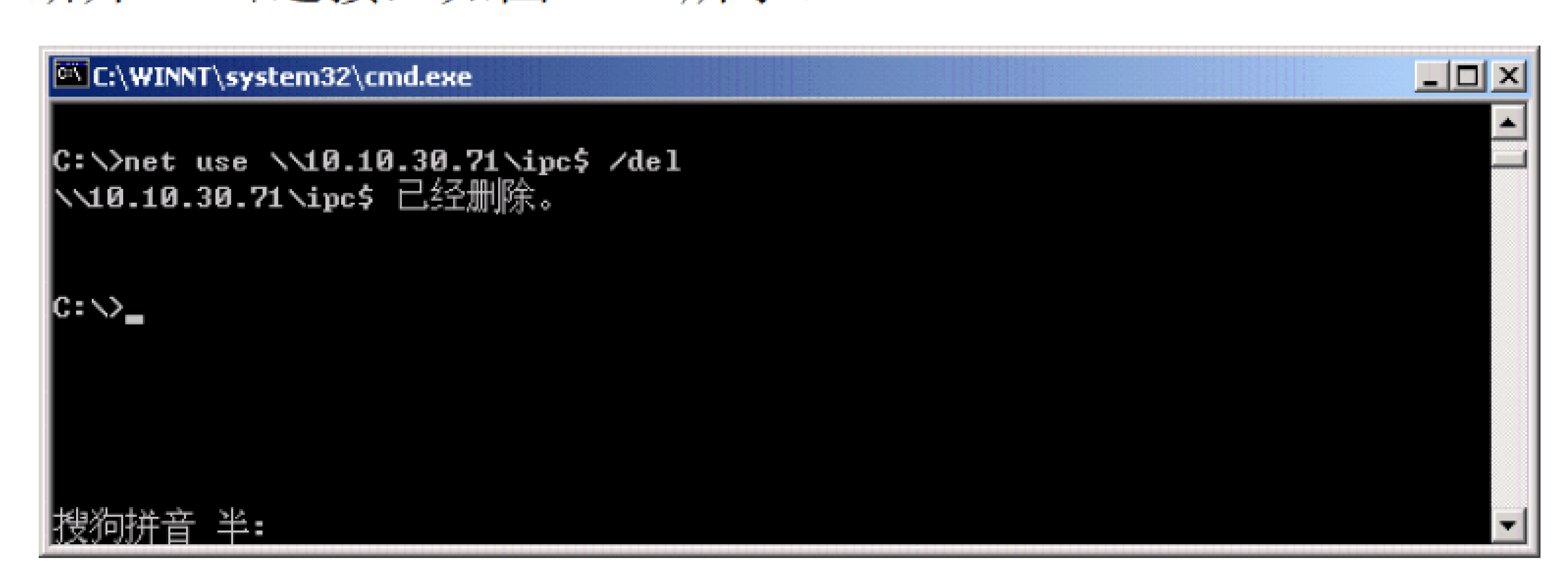


图 3.10　断开 IPC$连接

第 4 步：在本地计算机上打开 MS-DOS 界面，然后用该 MS-DOS 进行 Telnet 登录，如图 3.11 所示。

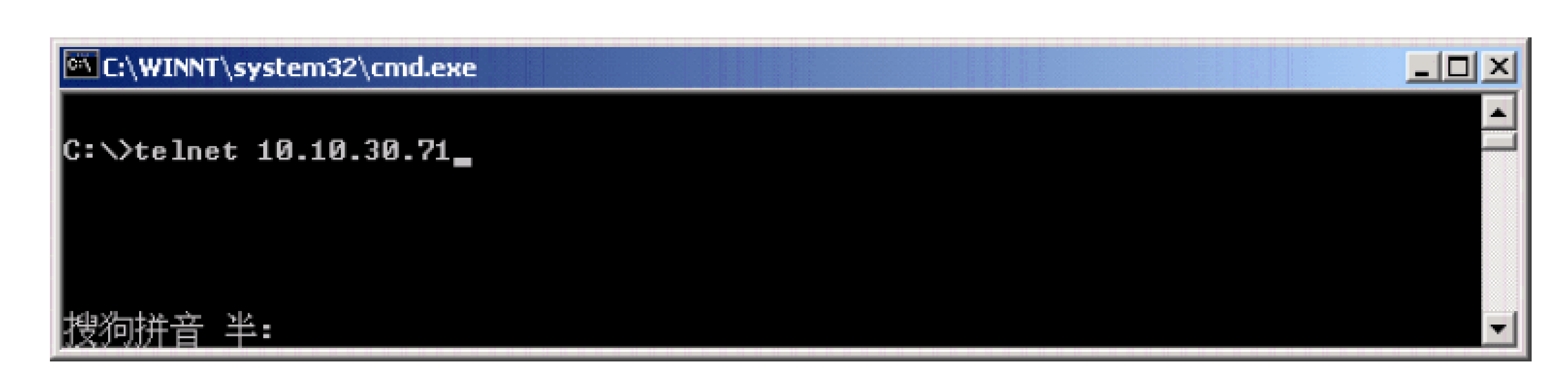


图 3.11　Telnet 登录

第 5 步：输入 telnet 10.10.30.71 命令并按 Enter 键后，在得到的界面中输入 y 表示发送密码并登录，如图 3.12 所示。如图 3.13 所示为登录成功后的界面。



图 3.12　在得到的界面中输入 y

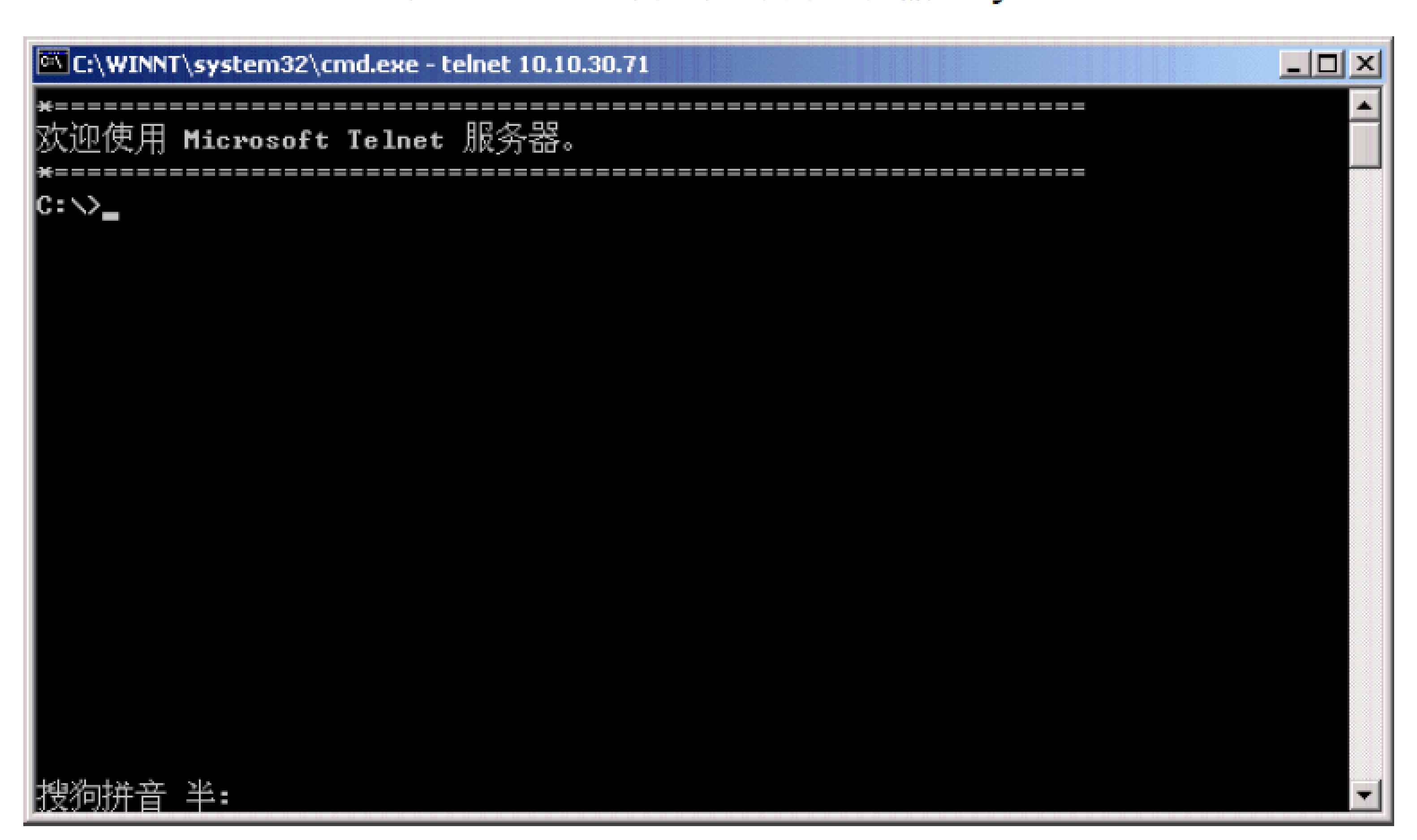
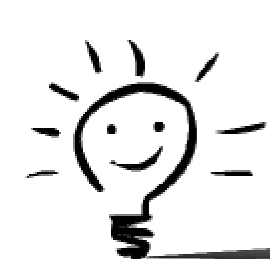


图 3.13　登录成功后的界面



第 6 步：如图 3.13 所示为远程主机为 Telnet 终端用户打开的 Shell，在该 Shell 中输入的命令将会直接在远程计算机上执行。比如，输入 net user 命令来查看远程主机上的用户列表，如图 3.14 所示。



图 3.14　查看远程主机上的用户列表

第 7 步：防范方法：禁用 Telnet 服务。在服务列表中找到 Telnet，双击打开 Telnet 服务的属性窗口，将该服务的启动类型设置为“禁用”。平时禁用该服务，需要时启动。

第 4 章 Windows Server 2003 网络安全与策略

知识目标

- 了解 Windows Server 2003 系统新增加的安全功能。
- 熟悉 Windows Server 2003 中的用户管理及其策略。
- 熟悉 Windows Server 2003 的文件访问权限及其策略。
- 熟悉 Windows Server 2003 中的资源审核。

技能目标

- 掌握 Windows Server 2003 中的用户管理及其策略。
- 掌握 Windows Server 2003 的文件访问权限及其策略设置。
- 掌握 Windows Server 2003 中的资源审核的方法。
- 掌握 Windows Server 2003 中安全使用数字证书的方法。

Windows Server 2003 已经成为目前 Windows 主流服务平台。本章主要介绍与 Windows Server 2003 有关的安全机制以及涉及 Windows Server 2003 系统安全与策略的一些技巧。

4.1 Windows Server 2003 网络安全特性

随着 Microsoft 公司.NET 战略的不断推进，越来越多的服务器开始采用 Microsoft Windows Server 2003 作为其操作系统，提供 Web 服务、数据库服务和电子商务平台及其他各种程序应用等。为了保证 Web 服务、数据库服务和电子商务平台等各种应用、服务的安全，操作系统自然要提供很高的稳定性和安全性。Windows Server 2003 是在 Windows Server 2002 的基础上，依据.NET 架构进行构建，提供了更高、更好的安全性、稳定性和可伸缩性，为服务器提供了一个高效的结构平台。

4.1.1 Windows Server 2003 简介

随着 Internet 的发展，企业已经越来越依赖 Internet 来发展自己。企业内部的 Intranet 已经与 Internet 互联，同时，Internet 规模也越来越大，繁重的商务活动要求企业的 Intranet 必须可靠、高效，更加安全。Windows Server 2003 系统提供的服务能够创建更安全可靠的环境。

1. Windows Server 2003 的优点

Windows Server 2003 作为 Windows 服务器产品，其主要优点表现在如下几个方面。

（1）可靠。Windows Server 2003 是最快、最可靠和最安全的 Windows 服务器操作系统之一。它提供集成结构，用于确保商务信息的安全性；提供可靠性、可用性和可伸缩性，提供用户需要的网络结构。

（2）高效。Windows Server 2003 提供各种工具，允许用户部署、管理和使用网络结构以获得最大效率。它提供灵活易用的工具，有助于使用户的设计和部署与单位和网络的要求相匹配；通过加强策略、使任务自动化及简化升级来帮助用户主动管理网络；通过让用户自行处理更多的任务来降低支持开销。

（3）联网。Windows Server 2003 可以帮助用户创建业务解决方案结构，以便与雇员、合作伙伴、系统和用户更好地沟通。它提供集成的 Web 服务器和流媒体服务器，帮助用户快速、轻松和安全地创建动态 Intranet 和 Internet Web 站点；提供集成的应用程序服务器，帮助用户轻松地开发、部署和管理 XML Web 服务；提供多种工具，使用户得以将 XML Web 服务与内部应用程序、供应商和合作伙伴连接起来。

（4）经济。与来自 Microsoft 公司的许多硬件、软件和渠道合作伙伴的产品和服务相结合，Windows Server 2003 提供了有助于使用户的结构投资获得最大回报的选择。它提供简单易用的说明性指南；通过利用最新的硬件、软件和方法来优化服务器部署，从而帮助用户合并各个服务器；降低用户的所属权总成本（TCO），使投资很快就能获得回报。

2. Windows Server 2003 的核心技术

Windows Server 2003 依据.NET 架构，包含了基于 Windows Server 2000 构建的核心技术，从而提供了经济的优质服务器操作系统。Windows Server 2003 的核心技术使机构和员工工作效率更高，并且能更好地沟通。其核心技术包括下列内容。

（1）可靠性。

Windows Server 2003 的可靠性通过可用性、可伸缩性和安全性来体现，使其成为高度可靠的平台。

① 可用性。Windows Server 2003 系统增强了集群支持，从而提高了其可用性。对于部署业务关键的应用程序、电子商务应用程序和各种业务应用程序的单位而言，集群服务是必不可少的，因为这些服务大大改进了单位的可用性、可伸缩性和易管理性。在 Windows Server 2003 中，集群安装和设置更容易也更可靠，而该产品增强的网络功能，提供了更强的故障转移能力和更长的系统运行时间。Windows Server 2003 系统支持多达 8 个节点的服务器集群。如果集群中某个节点由于故障或维护而不能使用，另一节点会立即提供服务，这一过程即为故障转移。Windows Server 2003 还支持网络负载平衡（NLB），它在集群中各个节点之间平衡传入 Internet 协议（IP）通信。

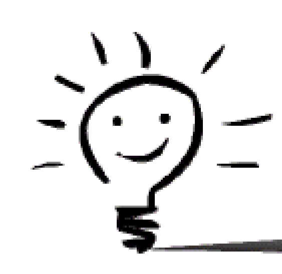
② 可伸缩性。Windows Server 2003 系统通过由对称多处理（SMP）支持的向上扩展和由集群支持的向外扩展来提供可伸缩性。内部测试表明，与 Windows Server 2000 相比，Windows Server 2003 在文件系统方面提高了性能（提高了 140%），其他功能（包括 Microsoft Active Directory 服务、Web 服务器和终端服务器组件以及网络服务）的性能也显著提高。Windows Server 2003 从单处理器解决方案扩展到 32 路系统，同时支持 32 位和 64 位处理器。

③ 安全性。通过 Intranet、Extranet 和 Internet 结合起来，各公司超越了传统的局域网（LAN）。因此，系统安全问题比以往任何时候都更为严峻。通过用户使用反馈及技术支持，Microsoft 公司修正了大量安全缺陷和错误。Windows Server 2003 在安全性方面提供了许多重要的新功能和改进方法，首先是包括一个公共语言运行库，这个软件引擎是 Windows Server 2003 的关键部分，它提高了可靠性，并有助于保证计算环境的安全。它降低了错误数量，并减少了由常见的编程错误引起的安全漏洞，因此，攻击者能够利用的弱点就更少了。公共语言运行库还验证应用程序是否可以无错误运行，并检查适当的安全性权限，以确保代码只执行适当的操作。同时，Microsoft 公司在新版操作系统中也升级了互联网信息服务器（Internet Information Services，IIS，目前是 8.0 版本），极大地增强了 Web 服务器的安全性，IIS6.0 在交付时的配置可获得最大安全性。IIS6.0 和 Windows Server 2003 提供了最可靠、最高效、连接最通畅以及集成度最高的 Web 服务器解决方案，该方案具有容错性、请求队列、应用程序状态监控、自动应用程序循环、高速缓存以及其他更多功能。这些功能是 IIS8.0 中许多新功能的一部分，它们使用户得以在 Web 上安全地执行业务。

（2）高效率。

Windows Server 2003 在许多方面都具有使机构和雇员提高工作效率的能力，主要包括如下几个方面。

① 文件和打印服务器。任何 IT 机构的核心都要求对文件和打印资源进行有效的管理，



同时又允许用户安全地使用。随着网络的扩展，位于站点上或远程位置甚至合伙公司中的用户增加了，管理员面临着不断增长的沉重负担。Windows Server 2003 系统提供了智能的文件和打印服务，其性能和功能都得到提高，从而使用户得以降低总拥有成本。

② Active Directory。Active Directory 是 Windows Server 2003 系统的目录服务。它存储了有关网络上对象的信息，并且通过提供目录信息的逻辑分层组织，使管理员和用户易于找到该信息。Windows Server 2003 对 Active Directory 做了不少改进，使其使用起来更通用、更可靠，也更经济。在 Windows Server 2003 中，Active Directory 提供了增强的性能和可伸缩性，它允许更加灵活地设计、部署和管理单位的目录。

③ 管理服务。随着桌面计算机、便携式计算机和便携式设备上计算量的递增，维护分布式个人计算机网络的实际成本也显著增加了。通过自动化来减少日常维护是降低操作成本的关键。Windows Server 2003 新增了几套重要的自动管理工具来帮助实现自动部署，包括 Microsoft 软件更新服务（SUS）和服务器配置向导。新的组策略管理控制台（GPMC）使管理组策略更加容易，从而使更多的机构能够更好地利用 Active Directory 服务及其强大的管理功能。此外，命令行工具使管理员可以从命令控制台执行大多数任务。GPMC 并不包括在 Windows Server 2003 中，而是作为一个独立的组件出售。

④ 存储服务。Windows Server 2003 在存储管理方面引入了新的增强功能，这使管理及维护磁盘和卷、备份和恢复数据以及连接存储区域网络（SAN）更为简易和可靠。

⑤ 终端服务器。Windows Server 2003 的终端服务组件构建在 Windows Server 2000 终端组件中可靠的应用服务器模式之上。终端服务可以将基于 Windows 的应用程序或 Windows 桌面本身传送到几乎任何类型的计算设备上，包括那些不能运行 Windows 的设备。

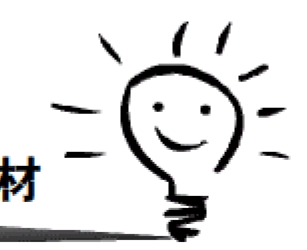
（3）联网能力。

Windows Server 2003 包含许多新功能，以确保用户所在的组织和用户本身保持连接状态，主要有以下几点。

① XML Web 服务。IIS6.0 是 Windows Server 2003 系统的重要组件。管理员和 Web 应用程序开发人员需要一个快速、可靠的 Web 平台，并且它是可扩展的和安全的。IIS 中的重大结构改进包括一个新的进程模型，它极大地提高了可靠性、可伸缩性和性能。默认情况下，IIS 以锁定状态安装，安全性得到了提高，因此系统管理员要根据应用程序要求来启用或禁用系统功能。此外，对直接编辑 XML 源数据库的支持改善了管理能力。

② 联网和通信。对于面临全球市场竞争挑战的单位来说，联网和通信是当务之急。员工需要在任何地点、使用任何设备接入网络。合作伙伴、供应商和网络外的其他机构需要与关键资源高效地交互，而且安全性比以往任何时候都重要。Windows Server 2003 系统的联网改进和新增功能扩展了网络结构的多功能性、可管理性和可靠性。

③ Enterprise UDDT 服务。Windows Server 2003 包括 Enterprise UDDI 服务，它是 XML Web 服务的动态而灵活的结构。这种基于标准的解决方案使公司能够运行他们自己的内部 UDDI 服务，以供 Intranet 和 Extranet 使用。开发人员能够轻松而快速地找到并重用单位内可用的 Web 服务。IT 管理员能够编录并管理他们网络中的可编程资源。利用 Enterprise UDDT 服务，公司能够生成和部署更智能、更可靠的应用程序。



④ Windows 媒体服务。Windows Server 2003 包括业内最强大的数字流媒体服务。这些服务是 Microsoft Windows Media 技术平台下一个版本的一部分，该平台还包括新版的 Windows 媒体播放器、Windows 媒体编辑器、音频视频编码解码器以及 Windows 媒体软件开发工具包。

（4）可拥有成本低。

由于 PC 技术提供了最经济的芯片平台，仅依靠 PC 就可完成任务已成为采用 Windows Server 2003 的重要经济动机。使用 Windows Server 2003 中自带的许多重要服务和组件，各机构可以迅速部署、管理和使用集成平台。

（5）XML Web 服务和.NET。

Microsoft.NET 已与 Windows Server 2003 系统紧密集成。它使用 XML Web 服务使软件集成程度达到了前所未有的水平：分散、模块化的应用程序通过 Internet 互相连接，并与其他大型应用程序相连接。通过集成到构成 Microsoft 平台的产品中，.NET 提供了通过 XML Web 服务迅速可靠地构建、托管、部署和使用安全的联网解决方案的能力。Microsoft 平台提供了一套联网所需的开发人员工具、用户端应用程序、XML Web 服务和服务器。这些 XML Web 服务提供了基于行业标准构建的可再次使用的组件，这些组件调用其他应用程序的功能。调用的方法独立于创建应用程序、操作系统、平台或设备用于访问它们的方法。利用 XML Web 服务，开发人员可以在企业内部集成应用程序，并跨网络连接合作伙伴和用户。这种先进的软件技术使合作成为可能，并且所带来的更有效的商业到商业和商业到用户的服务，可以对企业收入产生潜在的重要影响。数百万其他用户可以以各种组合使用这些组件。

3. Windows Server 2003 的安全功能

基于上述的各项核心技术，Windows Server 2003 系统新增了以下多项安全功能。

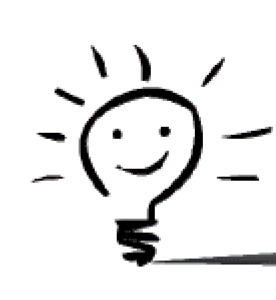
（1）授权管理器。授权管理器为应用程序开发人员提供了一个灵活框架，可将基于角色的访问控制集成到应用程序中，而且它为那些使用这些应用程序的管理员提供一种自然、直观的访问方式。授权管理器提供了可将基于角色的访问控制集成到应用程序的灵活的框架。它让使用这些应用程序的管理员，可提供对那些与作业功能相关的已分配用户角色进行访问的权限。授权管理器应用程序可以将授权策略存储为授权存储（存储在 Active Directorv 或 XML 文件中）的形式，而且可在运行时应用授权策略。

（2）存储用户名和密码。它是 Windows Server 2003 系统的一项功能，用于存储服务器的用户名和密码。该功能允许用户连接服务器时使用的用户名和密码与登录网络时使用的用户名和密码不同。用户可以存储这些用户名和密码以备将来再使用。

（3）软件限制策略。它使管理员可防止软件应用程序基于软件的哈希算法、软件的相关文件路径、软件发行者的证书或寄宿该软件的 Internet 区域来运行。使用软件限制策略，可以标识软件并控制它在本地计算机、组织单位、域或站点中的运行能力。

（4）证书颁发机构。证书颁发机构中含有大量的改进和新增的功能。

（5）受限委派。委派是允许服务模拟用户账户或计算机账户以便访问网络中的资源的操作。如果服务是“受信任委派”，则该服务可以模拟用户使用其他网络服务。通过这一新



的安全功能，可指定要信任的服务用以委派服务器。

（6）有效权限工具。它计算指定用户或组授予的权限。该计算考虑组成员身份生效的权限，以及从父对象继承的任何权限。它将查找用户或组作为其成员的所有域和本地组。

（7）加密文件系统（EFS）。使用它可以加密保存在磁盘上的文件和目录。

（8）Everyone 成员身份。内置 Everyone 组包括 Authenticated Users 和 Guests，但不再包括 Anonymous 组的成员。

（9）基于操作的审核。它提供了更多描述性的审核事件，而且提供机会让使用者可以选择在审核对象访问时要审核的操作。

4.1.2 Windows Server 2003 安全概述

Windows Server 2003 系统的安全模型的主要功能是用户身份验证、访问控制及 Active Directory 目录服务。

1. 身份验证

身份验证指的是用于验证实体或对象是否与自己所声明的实体或对象相同的过程，包括确认信息的来源和完整性。身份验证是系统安全的一个基础方面，它将对尝试登录到域或访问网络资源的任何用户进行身份确认。身份验证包括下列两种方式。

（1）交互式登录：向用户的本地计算机或 Active Directory 账户确认用户的身份。

（2）网络身份验证：向用户尝试访问的任何网络服务确认用户的身份。要提供这种类型的身份验证，安全系统将包括下面这些身份验证机制：Kerberos V5、公钥证书、安全套接字层/传输层安全性（SSLiTLS）、摘要和 NTLM（与 Windows NT 4.0 系统兼容）。

Windows Server 2003 系统的身份验证是对所有网络资源的单一登录。单一登录允许用户使用一个密码或智能卡一次登录到域，然后向域中的任何计算机验证身份。尝试对用户进行身份验证时，可使用多种工业标准类型的身份验证，这将由多种因素来决定。表 4.1 列出了 Windows Server 2003 系统支持的身份验证类型。

表 4.1 Windows Server 2003 系统支持的身份验证类型

身份验证类型	描　　述
Kerberos V5 身份验证	与密码或智能卡一起使用以进行交互登录的协议，它也是对服务进行网络身份验证的默认方法
安全套接字层/传输层安全性（SSLiTLS）身份验证	用户尝试访问安全的 Web 服务器时将使用的协议
NTLM 身份验证	当客户端或服务器使用早期版本的 Windows 时将使用的协议
摘要式验证	摘要式验证将凭据作为 MD5 哈希或消息摘要在网络上传递
Passport 身份验证	Passport 身份验证是可提供单一登录服务的用户身份验证服务

单一登录使用户在访问网络上的资源时不必重复提供凭据。对于 Windows Server 2003 系统来说，用户访问网络资源时只需要验证一次，随后的身份验证对该用户而言是透明的。除此之外，Windows Server 2003 系统的身份验证还包括双因素的身份验证，例如智能卡。

2. 基于对象的访问控制

访问控制是批准用户、组和计算机访问网络上的对象的过程。访问控制的主要内容是权限、用户权利和对象审核。

（1）权限。权限定义了授予用户或组对某个对象或对象属性的访问类型。权限被应用到任何受保护的对象，例如文件、Active Directory 对象或注册表对象。权限可以授予任何用户、组或计算机。设置权限，就是为组和用户指定访问级别。例如，可以在打印机上设置类似的权限，使某些用户可以配置打印机，而其他用户只能使用其打印。

（2）用户权利。用户权利授予计算环境中的用户和组特定的特权和登录权利。

（3）对象审核。可以审核用户对对象的访问情况。可以使用事件查看器在安全日志中查看这些与安全相关的事件。

在 Windows Server 2003 系统中，通过用户身份验证，系统允许管理员控制对网上资源或对象的访问。管理员通过将安全描述符分配给存储在 Active Directory 中的对象来实现访问控制。安全描述符列出了允许访问对象的用户和组，以及分配给这些用户和组的特定权限。安全描述符还指定了为对象审核的不同访问事件。文件、打印机和服务都是对象的示例。通过管理对象的属性，管理员可以设置权限、分配所有权以及监视用户访问。

管理员不仅可以控制对特殊对象的访问，也可以控制对该对象特定属性的访问。例如，通过适当配置对象的安全描述符，用户可以被允许访问一部分信息，如只访问员工姓名和电话号码，而不能访问他们的家庭住址。安全描述符是一种数据结构，包含与受保护的对象相关联的安全信息。安全描述符包括有关对象所有者、能访问对象的人员及其访问方式以及受审核的访问类型等方面的信息。

3. Active Directory 目录服务

Active Directory 是基于 Windows 的目录服务。Active Directory 存储有关网络上对象的信息，并让用户和网络管理员可以使用这些信息。Active Directory 允许网络用户使用单个登录进程来访问网络中任意位置的许可资源。它为网络管理员提供了直观的网络层次视图和对所有网络对象的单点管理。这些对象通常包括共享资源，如服务器、卷、打印机、网络用户和计算机账户。

Active Directory 通过使用对象和用户凭据的访问控制，提供了对用户账户和组信息的保护存储。由于 Active Directory 不仅存储用户凭据，还存储访问控制信息，因此，登录到网络的用户将同时获得访问系统资源的身份验证和授权。例如，用户登录到网络时，安全系统通过存储在 Active Directory 上的信息来验证用户。然后，当用户试图访问网络上的服务时，系统检查由随机访问控制列表为这一服务定义的属性。

由于 Active Directory 允许管理员创建组账户，因此管理员可以更有效地管理系统的安全性。例如，通过调整文件属性，管理员可以允许组中的所有用户读取文件。

Windows Server 2003 系统通过登录验证以及目录中对象的访问控制，将安全性集成到 Active Directory 中。通过一次网络登录，管理员可管理整个网络中的目录数据和单位，而且获得授权的网络用户可访问网络上任何地方的资源。这种基于策略的管理减轻了即使是最复杂的网络管理。



4.2 Windows Server 2003 用户安全策略

Windows Server 2003 作为一款网络操作系统产品，其上有许多网络应用程序和服务在运行，Windows Server 2003 的安全，直接决定了这些应用程序和服务的安全，特别是在 Windows Server 2003 作为网络中的域控制器时，一旦发生安全事故，将使得整个域中的用户无法正常地进行用户身份验证，从而影响应用程序和服务的使用。怎样设置安全的域用户策略，使得域中用户正常访问网络，正是本节将要探讨的内容。

4.2.1 Windows Server 2003 账户策略和本地策略

在设置安全的用户策略前，首先来了解一下什么是安全设置和安全策略。在 Windows Server 2003 中，安全设置和安全策略是配置在一台或多台计算机上的规则，用于保护计算机或网络上的资源。安全设置可以控制下列几项内容。

（1）用户访问网络或计算机的身份认证方式。

（2）授权给用户的可以使用的资源。

（3）无论用户的或者组的操作都被记录在事件日志中。

（4）组成员。

在 Windows Server 2003 中，用户账户有两种，分别是本地用户和组、域用户和组。对于本地用户和组，将在 4.3 节中进行讨论，本节将详细介绍域用户和组及其安全策略的设置。

在 Active Directory 中，用户账户和计算机账户代表物理实体，如计算机或人。用户账户也可用作某些应用程序的专用服务账户。用户账户和计算机账户（以及组）也称为安全主体，是被自动指派了安全标识符（SID）（可用于访问域资源）的目录对象。用户或计算机账户用于下列几个方面。

（1）验证用户或计算机的身份。用户账户使用户能够利用经域验证后的标识登录到计算机和域。登录到网络的每个用户应有自己的唯一账户和密码。

（2）授权或拒绝访问域资源。一旦用户已经通过身份验证，那么就可以根据指派给该用户的关于资源的显式权限，授予或拒绝该用户访问域资源。

（3）管理其他安全主体。Active Directory 在本地域中创建外部安全主体对象，用以表示信任的外部域中的每个安全主体。

（4）审核使用用户或计算机账户执行的操作。审核有助于监视账户的安全性。

账户策略包含 3 个子集，分别如下。

（1）密码策略。用于域或本地用户账户，确定密码设置（如强制执行和有效期限）。

（2）账户锁定策略。用于域或本地用户账户，确定某个账户被系统锁定的情况和时间长短。

（3）Kerberos 策略。用于域用户账户，确定与 Kerberos 相关的设置（如票证的有效期



限和强制执行）。

对于域账户，只有一种账户策略。账户策略必须在“默认域策略”中定义，并且由组成该域的域控制器实施。域控制器始终从“默认域策略组策略对象”中获得账户策略，即使已经存在了一个应用到包括该域控制器在内的不同账户策略。默认情况下，加入到域（如成员计算机）中的工作站和服务器会接收到相同的账户策略，以用于本地账户。然而，本地账户策略可能不同于域账户策略，例如，当为各个本地账户定义账户策略时，即是如此。

在 Active Directory 中，每个域用户账户在建立时，都有许多账户选项可以选择，这些选项能够确定，如何在网上对持有特殊用户账户进行登录的人员实施身份验证。表 4.2 列出了这些账户选项。

表 4.2　域账户选项

账 户 选 项	描　述
用户下次登录时需更改密码	强制用户下次登录网络时更改密码
用户不能更改密码	阻止用户更改其密码
密码永不过期	防止用户密码过期
使用可逆的加密保存密码	允许用户从 Apple 计算机登录 Windows 网络
账户已禁用	防止用户使用选定的账户登录
交互式登录必须使用智能卡	要求用户拥有智能卡来交互地登录网络。用户还必须具有连接到其计算机的智能卡读取器以及智能卡的有效个人标识号（PIN）。当选择该选项时，用户账户的密码将被自动设置为随机且复杂的值，并设置“密码永不过期”选项
信任账户作为委派	允许在该账户下运行的服务代表网络中的其他用户账户执行操作；对于运行在受信任委派的用户账户（也称为服务账户）下的服务，可以模拟客户端以获取运行该服务的计算机或其他计算机上的资源的访问权；该选项仅可用于运行 Windows Server 2003 的域控制器（其中域功能被设置为 Windows 2000 混合模式或 Windows 2000 纯模式）。在运行 Windows Server 2003 的域控制器上（其中域功能级别被设置为 Windows Server 2003），使用“委派”选项卡来配置委派设置。仅对具有已指派 SPN 的账户，才显示“委派”选项卡
敏感账户，不能被委派	允许对用户账户进行控制，例如来宾账户或临时账户
此账户需要使用 DES 加密类型	提供对数据加密标准（DES）的支持
不要求 Kerberos 预身份验证	支持 Kerberos 协议的备用实现。运行 Windows 2000 或 Windows Server 2003 的域控制器，可使用其他机制来同步时间

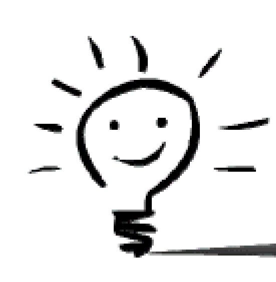
对于本地策略，这些策略主要应用于本地计算机，同样包含有 3 个子集。

（1）审核策略。确定是否将安全事件记录到计算机上的安全日志中。同时也确定是记录登录成功还是记录登录失败，或二者都记录。

（2）用户权限分配。确定具有登录本地计算机的权利或特权的用户或组。

（3）安全选项。启用或禁用计算机的安全设置。

对于本地策略，管理员应该要十分重视，因为它直接决定了服务器的安全。不安全的



本地策略将导致未经授权的使用者从本地非法登录，进而对域帐户及策略做出修改，从而导致整个网络出现帐户策略安全故障。执行“开始”→“运行”命令，在文本框中输入 gpedit.msc 以打开“组策略编辑器”窗口，依次展开“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”→“安全选项”文件夹，在其中进行本地策略的各种安全设置，如图 4.1 所示。双击其中的任何一个策略设置选项，将出现一个相应内容的对话框，要求操作者进行参数的输入或选择，管理员只需根据当前的安全策略来进行操作即可，如图 4.2 所示。

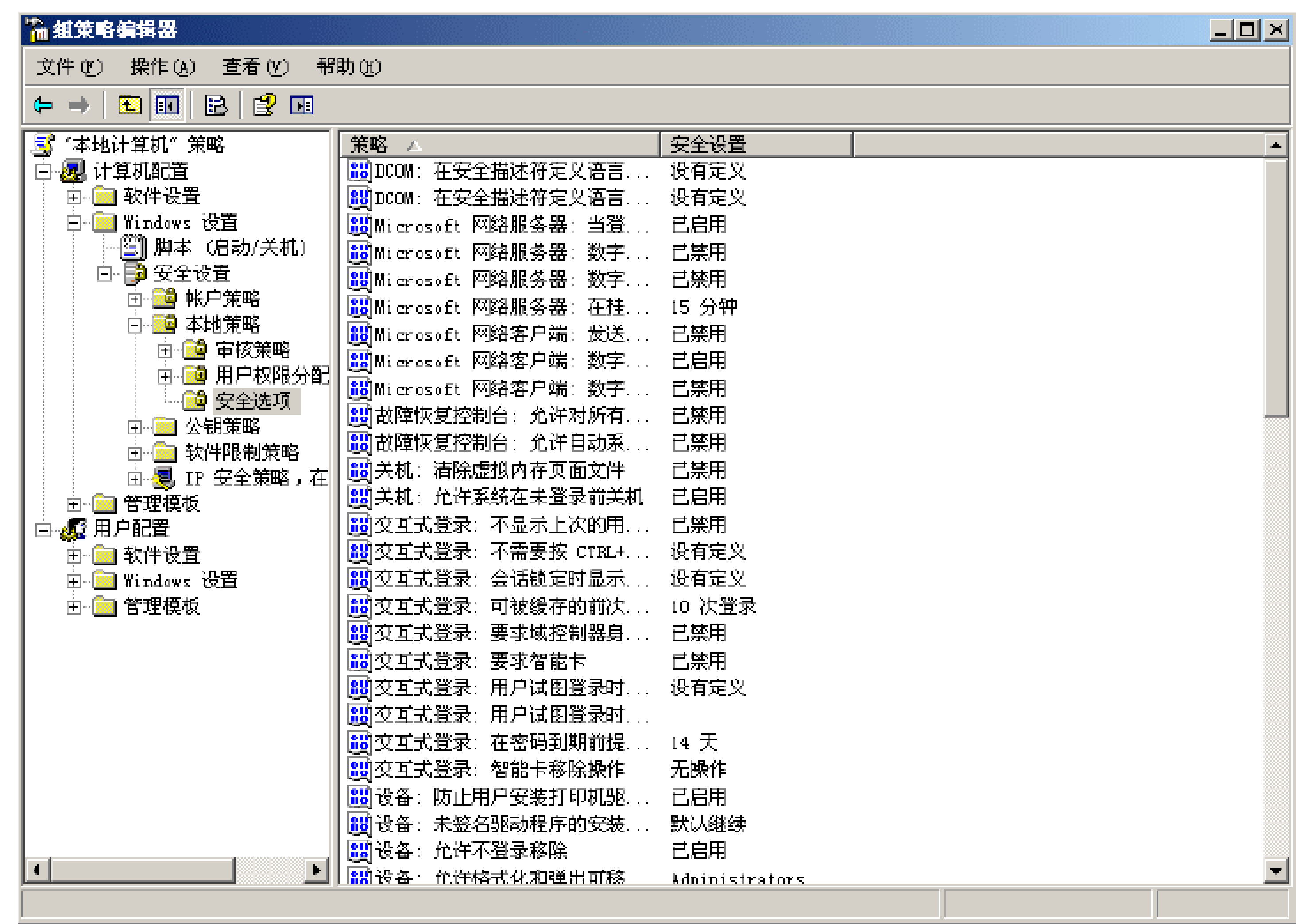


图 4.1 “组策略编辑器”窗口

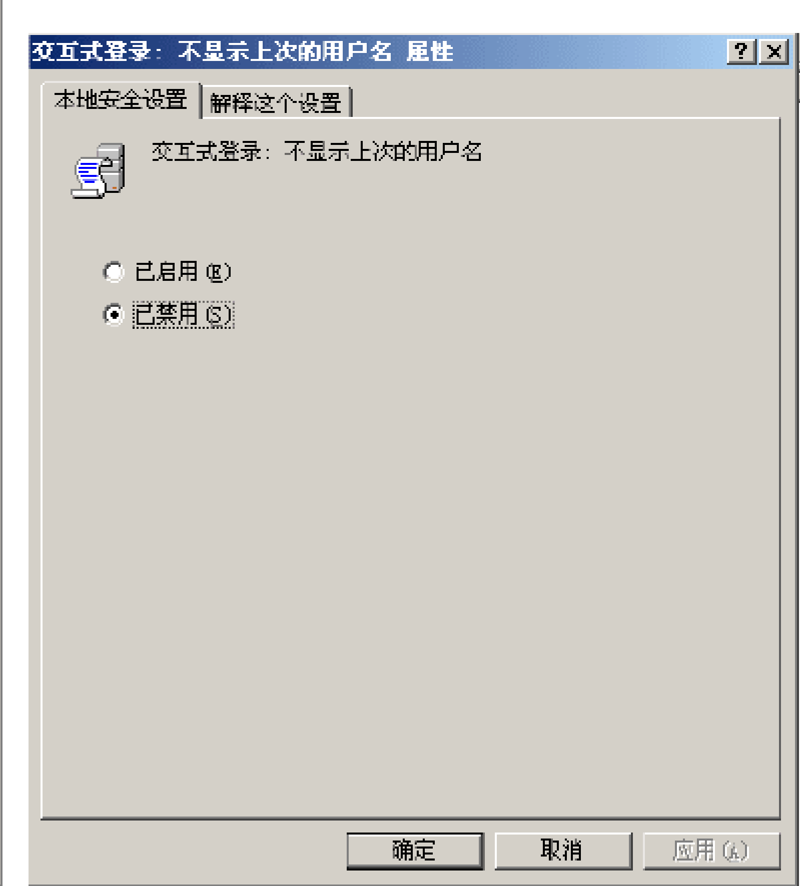


图 4.2 “交互式登录”对话框

4.2.2 Windows Server 2003 账号密码策略

当管理员在域中为每位网络用户设置账户时，通常会使用一个默认值来为这些域账户设置密码。当账户交付给用户后，用户能够自己来重新设置密码。但因为种种原因，用户自己设置的密码往往不符合密码安全规定，如密码过于简单、不够复杂等，这些都为网络安全带来隐患。在网络的使用过程中，用户可能会忘记自己的密码，这时需要管理员来进行用户密码的恢复，但不应对用户在域中的其他密码信息造成丢失。因此作为管理员，必须要了解在 Windows Server 2003 中有关密码的相关知识及其策略设置。

1. 安全密码

密码在保证企业网络安全中扮演的角色经常被低估甚至忽略。密码为抵御对企业网络的非法访问构筑了第一道防线。Windows Server 2003 可以在操作系统启动时检查 Administrator 账户密码的复杂程度。如果密码为空或者不满足复杂性要求，将会显示一个警告框，警告操作者 Administrator 账户不使用强密码可能存在危险，如果继续使用空密码，可能无法通过网络访问该账户。

弱密码会使得攻击者易于访问用户的计算机和网络，而强密码则难以破解，即使现在的密码破解软件越来越强大。当然，只要有足够时间，任何密码仍然能够被破解。即便如



此，破解强密码也远比破解弱密码困难得多。因此安全的计算机需要所有用户账户都使用强密码。对于强密码，一般都具有以下的特性。

（1）长度至少有 7 个字符。

（2）不包含用户名、真实姓名或公司名称。

（3）不包含完整的字典词汇。

（4）与先前的密码大不相同。

同时，强密码的组成全部包含下列 4 组字符类型。

（1）大写字母。

（2）小写字母。

（3）数字。

（4）键盘上的其他字符（键盘上所有未定义为字母和数字的字符）。

这 4 组字符毫无规律地排列在一起构成密码，例如 h*54p4e>F。

需要注意的是，有的密码虽然可以满足大多数强密码的条件，但仍然较弱。例如，love521!，就是一个相对而言的弱密码，即使它能够满足成为强密码的多数条件，也能够满足密码策略的复杂性要求。但因为这个密码的部分组成仍然是有规律的，容易被破解。Windows 密码长度最多为 127 个字符，但 Windows 98 支持的最大密码长度为 14 个字符。

2. 密码重设盘

用户时常会忘记自己的本地用户账户的密码，特别是在使用强密码的情况下。在密码重设盘出现前，管理员恢复被忘记的本地用户账户密码的唯一方法只有手动重设用户的密码。但该操作会造成以下信息的丢失。

（1）使用用户公钥加密的电子邮件。

（2）计算机中保存的 Internet 密码。

（3）由用户加密的文件。

密码重设盘为忘记本地用户账户密码的用户提供了另一种解决方案。如果用户在忘记密码前为自己的本地账户创建了密码重设盘，则可以重设密码，而不会丢失先前因管理员重设密码而丢失的宝贵数据。

在创建密码重设盘时，公钥和私钥会成对创建。私钥存储在磁盘，即密码重设盘中，由公钥加密本地用户账户密码。如果用户忘记了密码，则可以插入包含有私钥的密码重设盘来解密当前密码。“忘记密码向导”会提示用户输入新的密码，然后用公钥进行加密。这时数据将不会丢失，因为用户只是更改了密码而已。

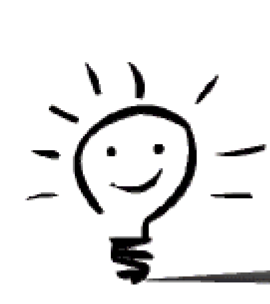
用户如何为自己的密码创建密码重设盘呢？很简单，下面的步骤将帮助用户创建密码重设盘（以用户使用 Windows XP 为例，Windows 2000/2003 系统是相同操作）。

（1）按 Ctrl+Alt+Del 组合键，在弹出的窗口中单击“更改密码”按钮。

（2）在“用户名”文本框中，输入要创建密码重设盘的账户的用户名。

（3）在“登录到”下拉列表框中选择输入的账户需要登录的计算机名称，然后单击“备份”按钮。

（4）按照“忘记密码向导”窗口中的步骤进行操作，直至完成操作。最后将密码重设盘保存在安全的地方。



3. 设置账户密码策略

密码策略作用于域账户或本地账户，包含以下几个方面。

☑ 强制密码历史。

☑ 密码最长使用期限。

☑ 密码最短使用期限。

☑ 密码长度最小值。

☑ 密码必须符合复杂性要求。

☑ 用可还原的加密来存储密码。

这些选项的配置方法均需根据当前用户账户类型来选择。默认情况下，成员计算机的配置与其域控制器的配置相同。为了保证所有用户创建的密码都符合管理员所设置的规则，管理员需要进行密码策略设置，它包括在域控制器上进行密码策略设置、在已加入域的成员服务器上进行密码策略设置，及在本地计算机上进行密码策略设置。

1）设置域控制器的密码策略

设置域控制器的密码策略的步骤如下。

（1）在控制台树中要设置组策略的域或组织单位上右击，在弹出的快捷菜单中选择“属性”命令，在弹出的对话框中选择“组策略”选项卡，选择列表框“组策略对象链接”中的项目以选择现有的组策略对象，然后单击“编辑”按钮，即可打开“组策略编辑器”窗口。也可单击“新建”按钮来创建新的组策略对象，然后再单击“编辑”按钮，也可打开“组策略编辑器”窗口，如图 4.3 所示。

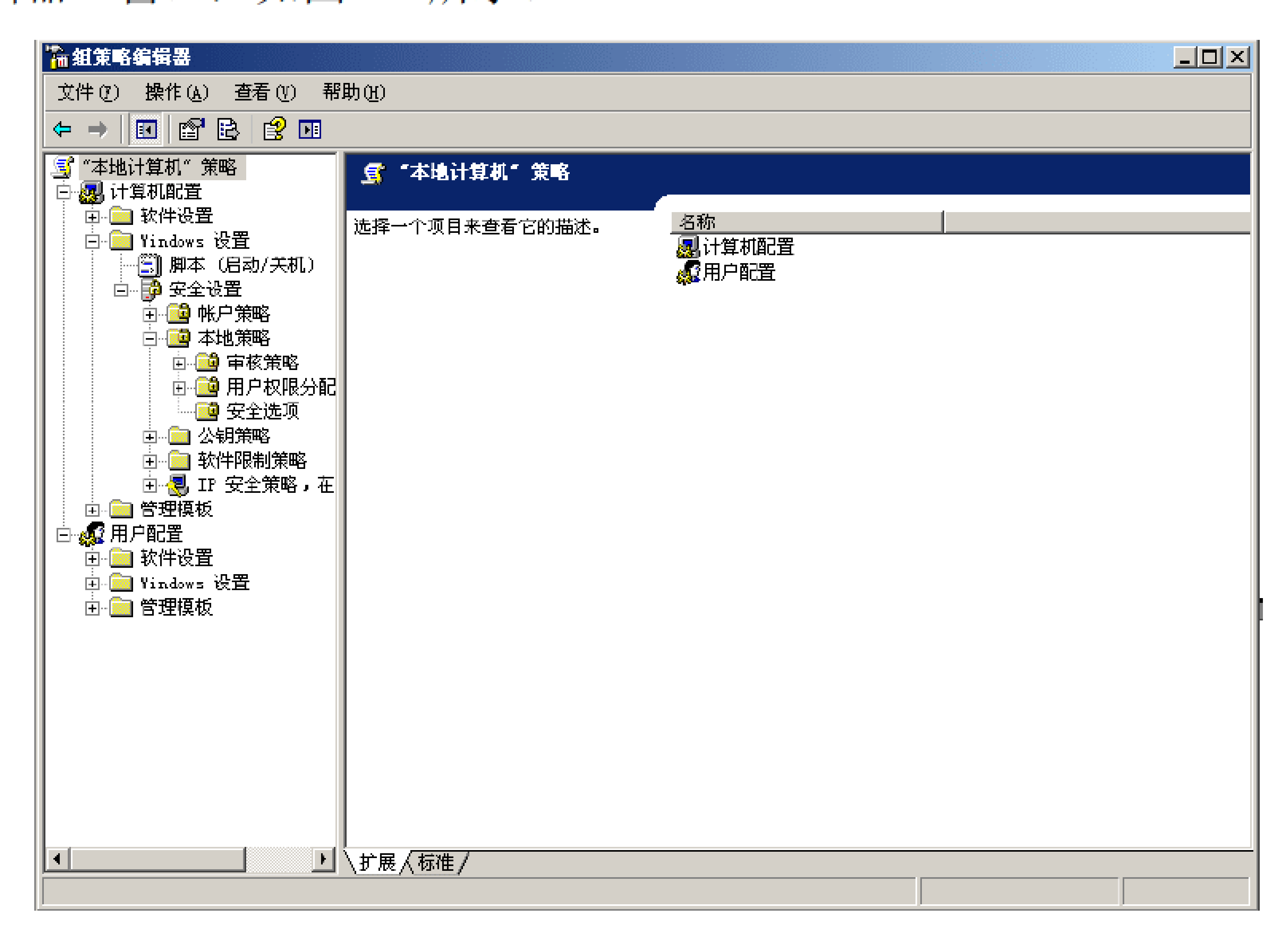
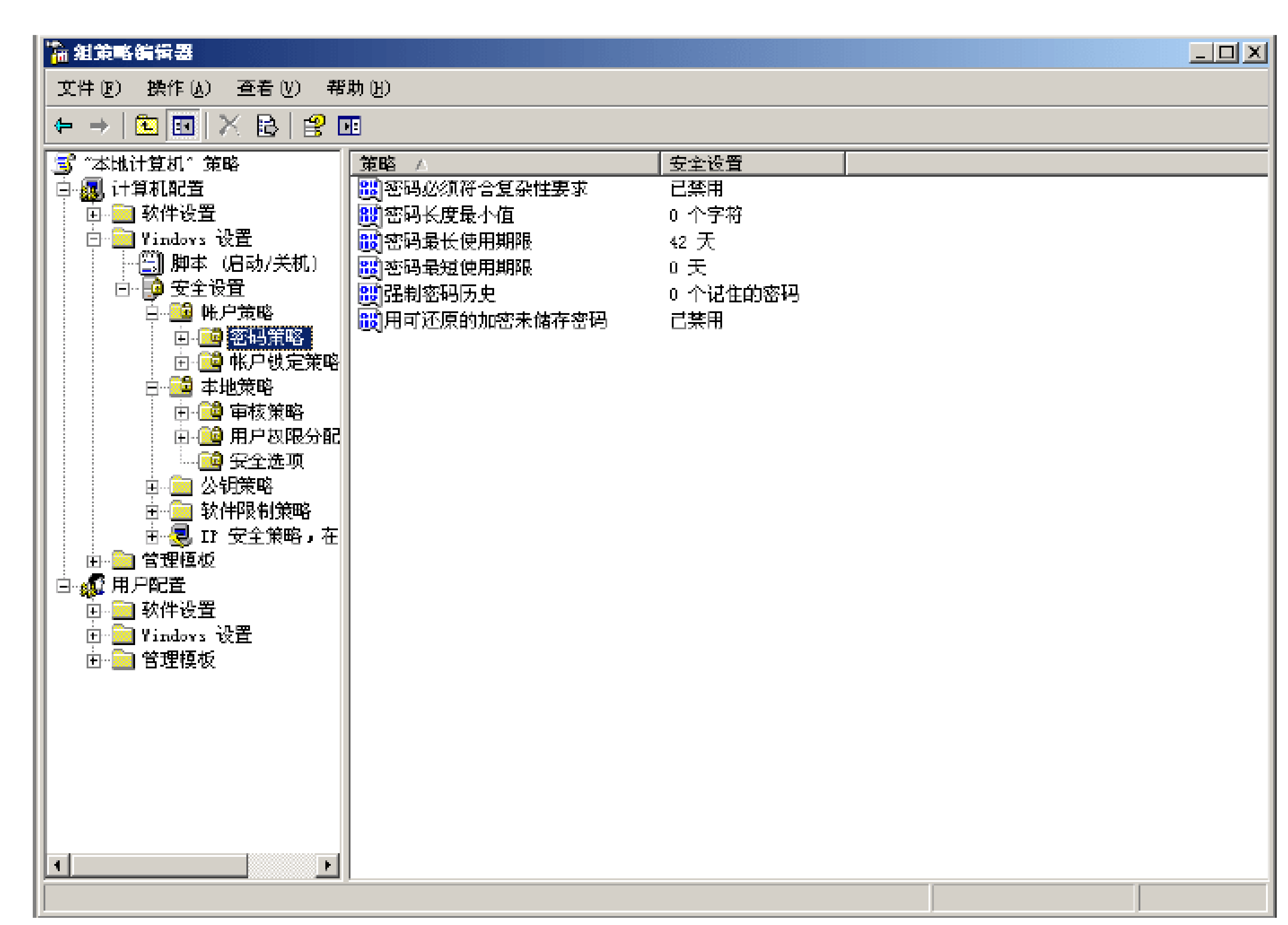


图 4.3 “组策略编辑器”窗口

（2）在控制台树中，展开“计算机配置”→“Windows 设置”→“安全设置”→“账户策略”→“密码策略”文件夹，在其中进行密码策略的各种安全设置，如图 4.4 所示。双击其中的任何一个密码策略设置选项，将出现一个相应内容的对话框，要求操作者进行参数的输入或选择，管理员只需根据当前的密码策略来进行操作即可，如图 4.5 所示。



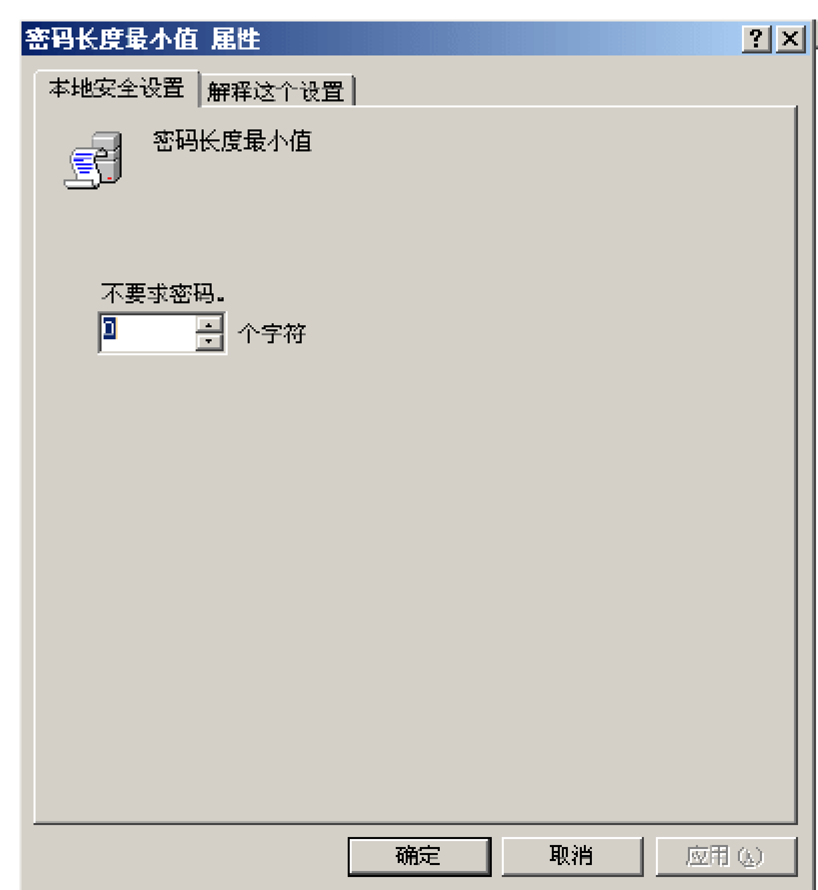


图 4.4　“密码策略”文件夹窗口　　　　图 4.5　“密码长度最小值 属性”对话框

2）设置域成员服务器或工作站的密码策略

对于这种情形，用户的本地密码策略配置方法如下。

（1）执行“开始”→“运行”命令，在“打开”文本框中输入 mmc 命令，打开“控制台 1”窗口，如图 4.6 所示。

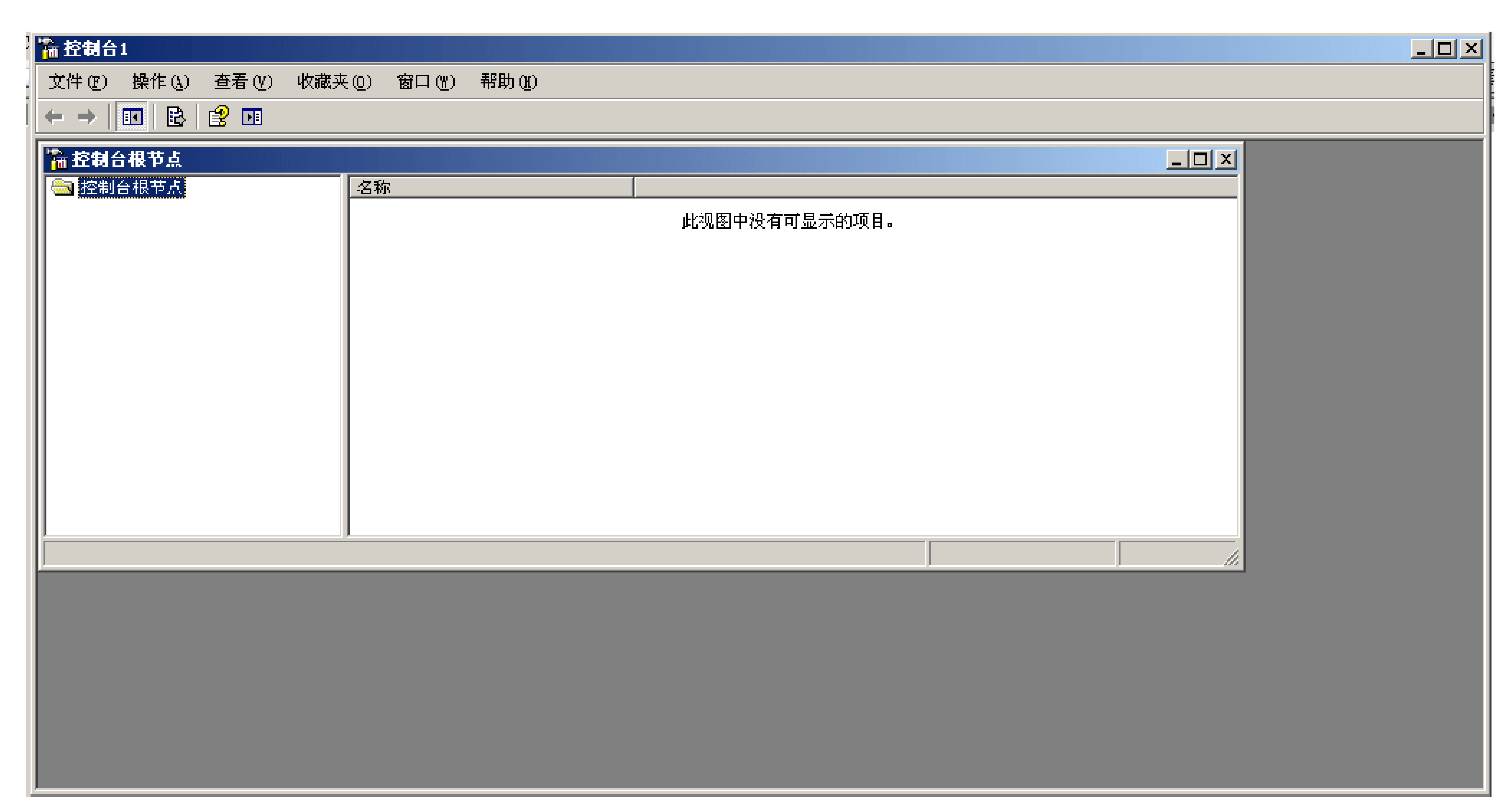
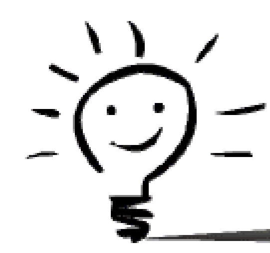
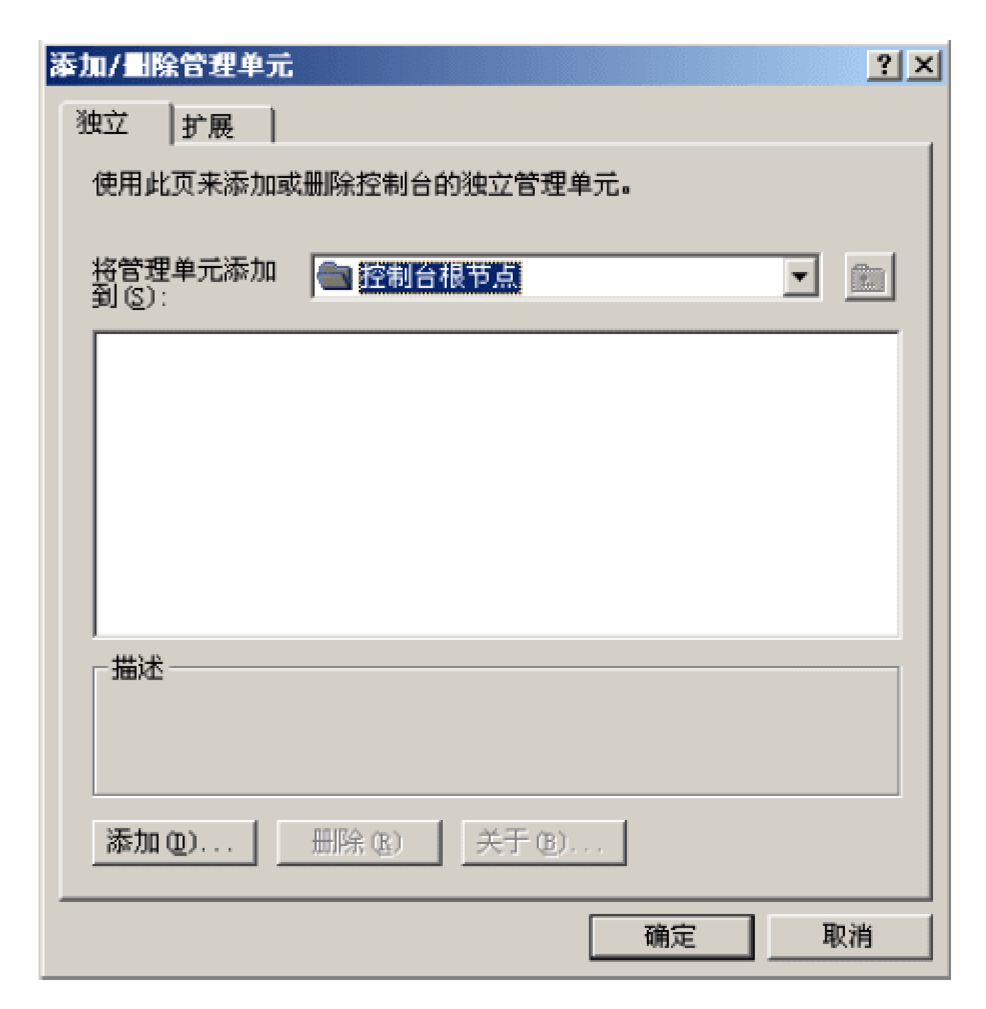


图 4.6　“控制台 1”窗口

（2）在该窗口中执行“文件”→“添加/删除管理单元”命令，弹出如图 4.7 所示的对话框。在该对话框中可以添加在控制台管理的管理单元。

（3）单击“添加”按钮，弹出“添加独立管理单元”对话框，如图 4.8 所示。在该对话框中双击“组策略对象编辑器”选项，或单击选择它后再单击“添加”按钮，弹出“选择组策略对象”对话框，如图 4.9 所示。在该对话框中要求选择所添加的组策略对象编辑器所作用的对象。







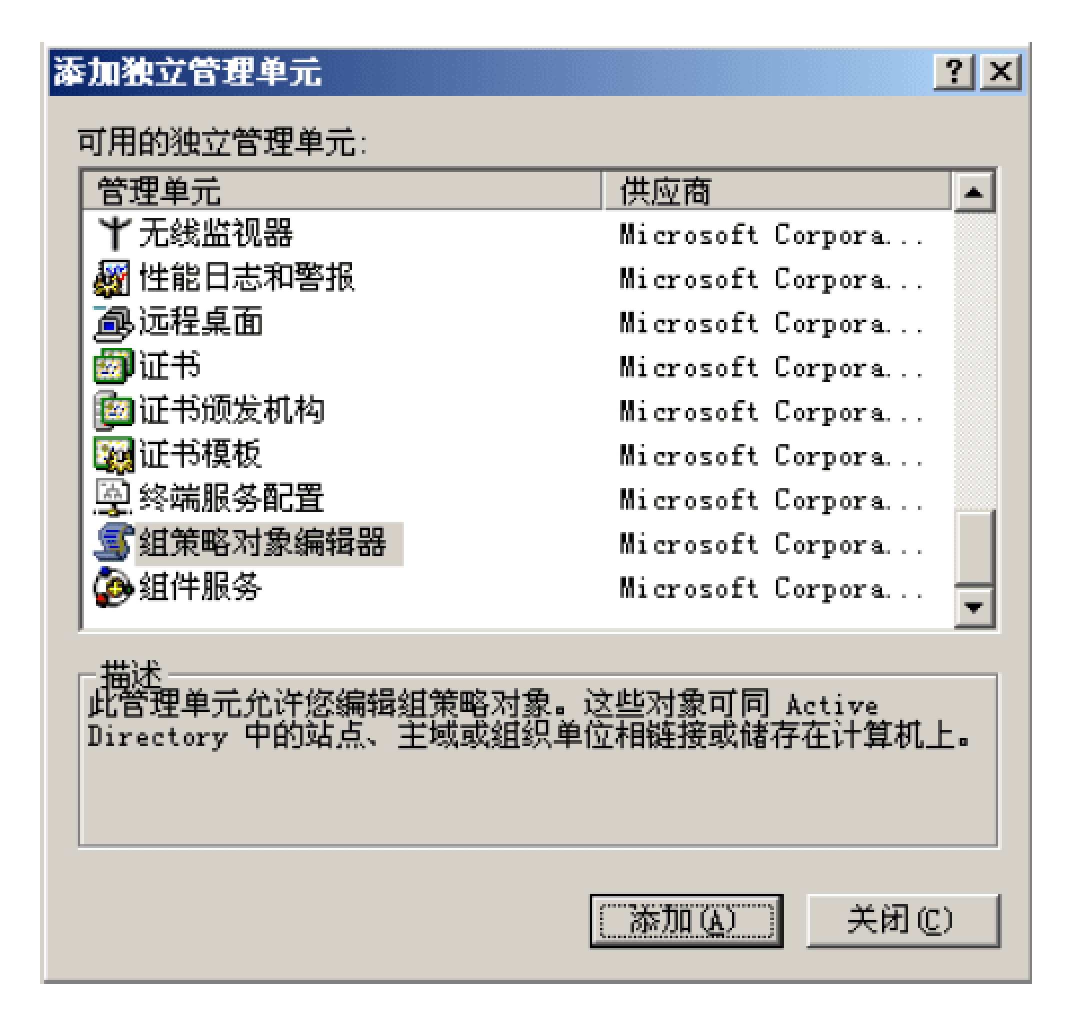


图 4.7 “添加/删除管理单元”对话框　　　图 4.8 “添加独立管理单元”对话框

因为是设置成员服务器或工作站（非本地计算机）的密码策略，所以单击“浏览”按钮，打开“浏览组策略对象”对话框，如图 4.10 所示。在该对话框中选择“计算机”选项卡，然后选中“另一台计算机”单选按钮，然后直接在下面的文本框中输入计算机 IP 地址或再次通过单击“浏览”按钮，打开对话框查找。



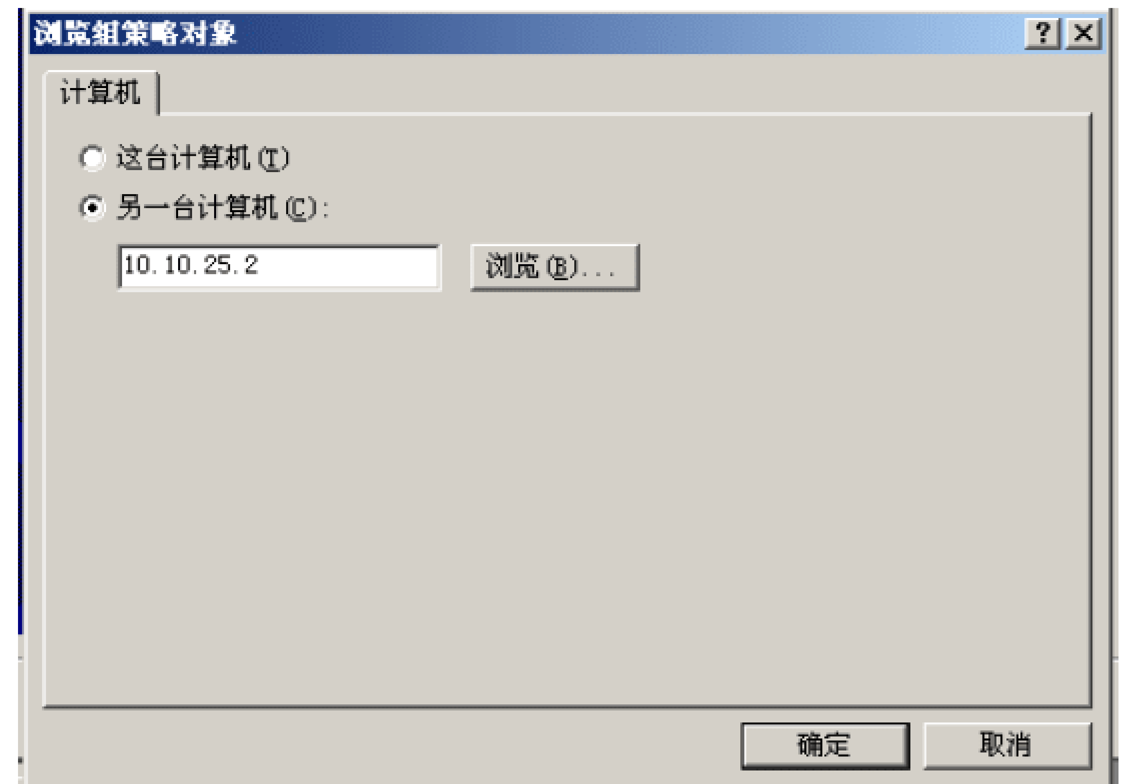


图 4.9 “选择组策略对象”对话框　　　图 4.10 “浏览组策略对象”对话框

（4）输入或者选择好计算机后，单击“确定”按钮返回到“选择组策略对象”对话框。单击“完成”按钮返回“添加独立管理单元”对话框，如果所选择的成员服务器或工作站与当前服务器的网络连接正常的话，即可把它们指派到组策略对象编辑器中。

（5）单击“添加独立管理单元”对话框中的“关闭”按钮，返回到“添加/删除管理单元”对话框，这时可以看到刚刚添加的组策略已经显示出来了，如图 4.11 所示，单击“确定”按钮返回到控制台窗口。

（6）依次单击展开“计算机配置”→“Windows 设置”→“安全设置”→“账户策略”→“密码策略”文件夹，然后在右边详细信息窗口中选择相应的密码策略选项配置即可。



配置方法也是在相应选项上右击，在弹出的快捷菜单中选择“属性”命令，操作方法同前，参照即可。

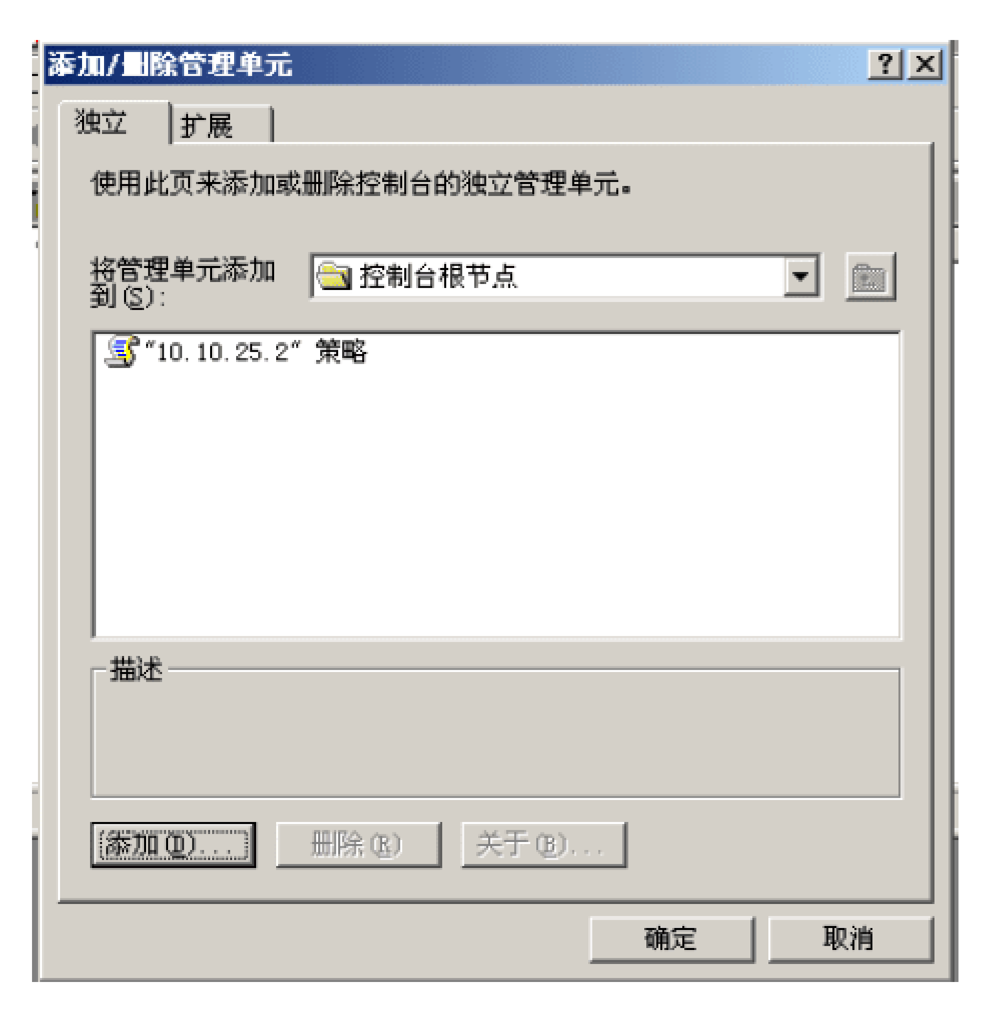


图 4.11　“浏览组策略对象”对话框

3）设置本地的密码策略

对于本地计算机的用户账户，其密码策略设置是在“本地安全设置”管理工具中进行的，其操作步骤如下。

（1）执行“开始”→“运行”命令，在“打开”文本框中输入 gpedit.msc，单击“确定”按钮，打开“组策略编辑器”窗口，如图 4.12 所示。

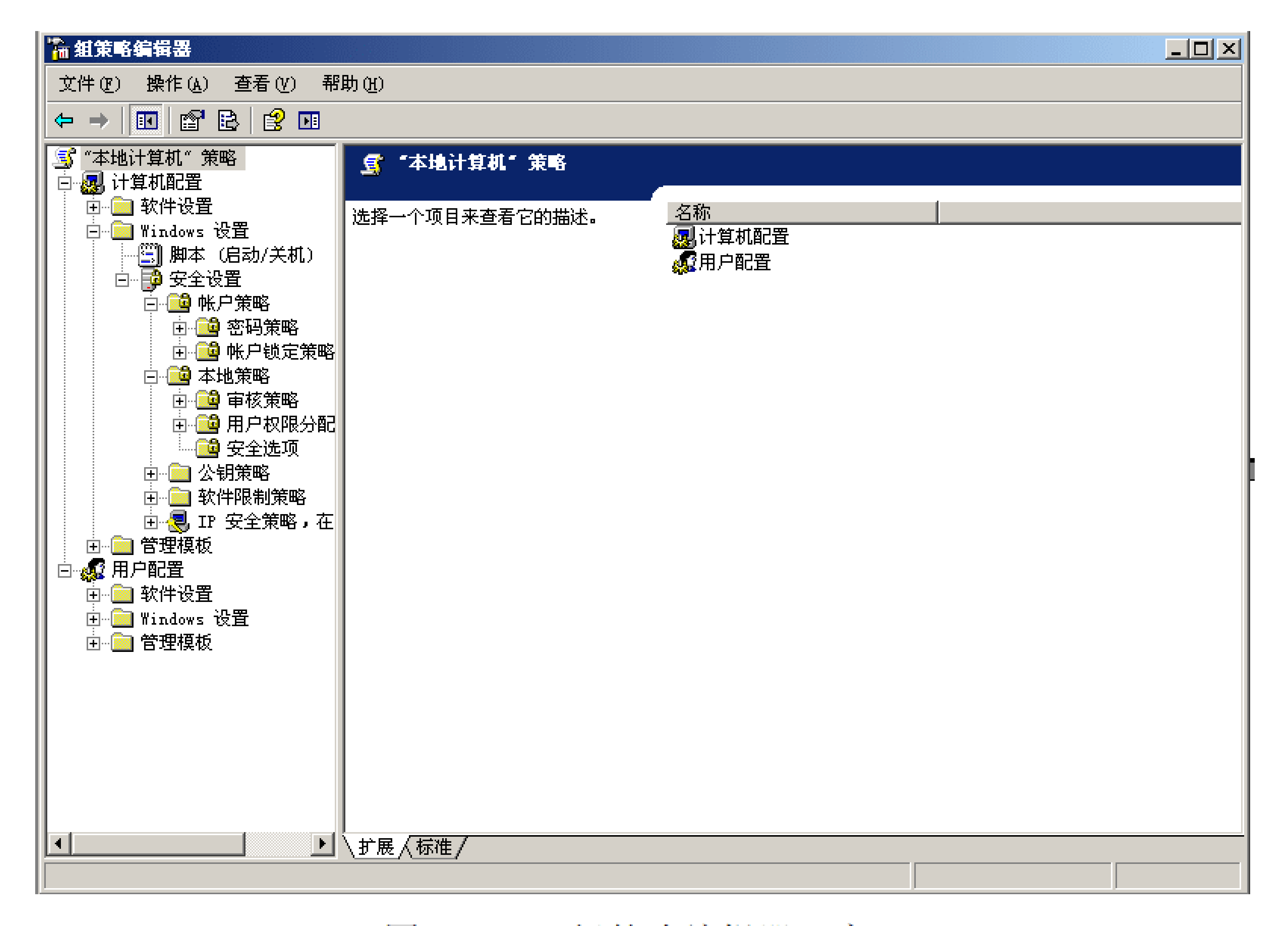


图 4.12　“组策略编辑器”窗口

（2）依次展开“计算机配置”→“Windows 设置”→“安全设置”→“账户策略”→“密码策略”文件夹，在其中进行本地密码策略的各种安全设置，如图 4.13 所示。双击其中的任何一个密码策略设置选项，将出现一个相应内容的对话框，要求操作者进行参数的



输入或选择，管理员只需根据当前的密码策略来进行操作即可，如图 4.14 所示。

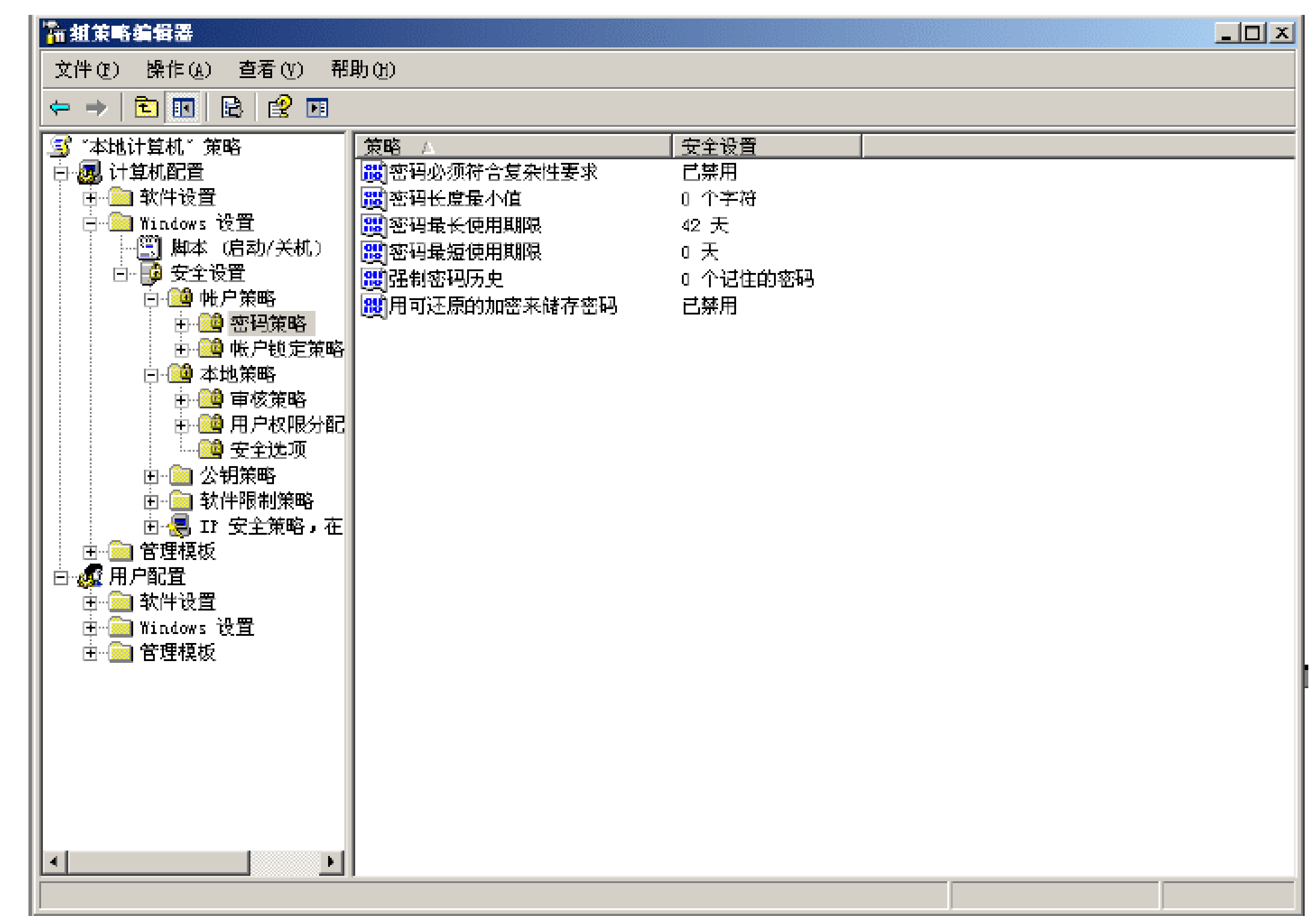


图 4.13 “密码策略”文件夹

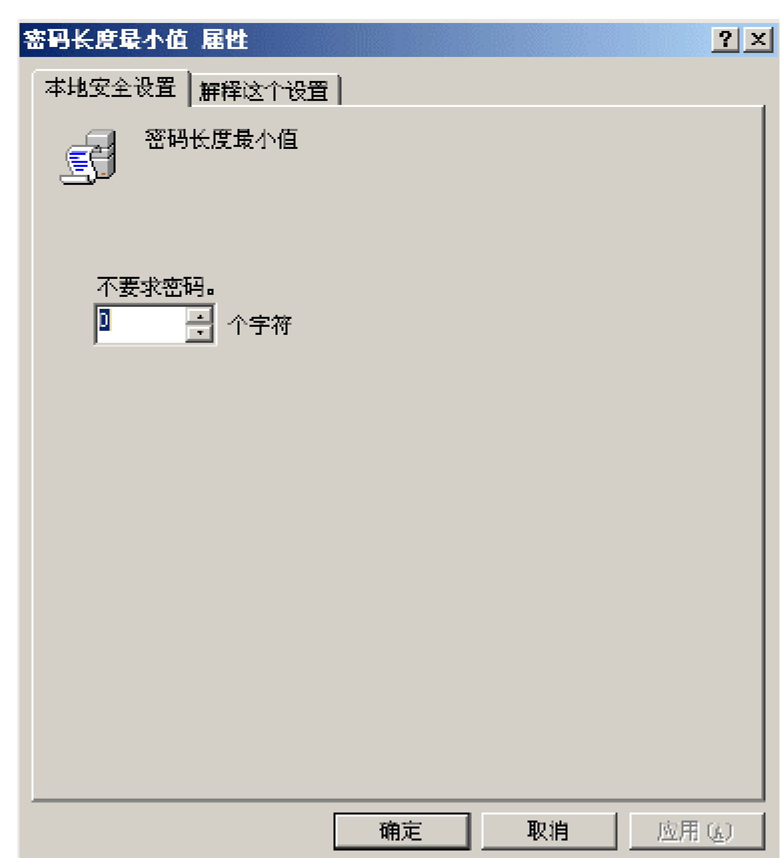


图 4.14 “密码长度最小值 属性”对话框

4）账户锁定策略

账户锁定策略用于域账户或本地用户账户，它们确定某个账户被系统锁定的情况和时间长短。主要包含以下 3 个方面。

（1）账户锁定时间。该安全设置确定锁定的账户在自动解锁前保持锁定状态的分钟数。有效范围从 0～99999 分钟。如果将账户锁定时间设置为 0，那么在管理员明确将其解锁前，该账户将被锁定。如果定义了账户锁定阈值，则账户锁定时间必须大于或等于重置时间，默认值为无。因为只有当指定了账户锁定阈值时，该策略设置才有意义。

（2）账户锁定阈值。该安全设置确定造成用户账户被锁定的登录失败尝试的次数，账号被锁定后将无法使用，除非管理员进行了重新设置或该账户的锁定时间已过期。登录尝试失败的范围可设置为 0～999 之间。如果将此值设为 0，则将无法锁定账户。对于使用 Ctrl+Alt+Del 组合键或带有密码保护的屏幕保护程序锁定的工作站或成员服务器计算机，失败的密码尝试计入失败的登录尝试次数中。默认值为 0。

（3）复位账户锁定计数器。该安全设置确定在登录尝试失败计数器被复位为 0（即 0 次失败登录尝试）之前，尝试登录失败之后所需的分钟数。有效范围为 1～99999 分钟。如果定义了账户锁定阈值，则该复位时间必须小于或等于账户锁定时间，默认值为无。因为只有当指定了账户锁定阈值时，该策略设置才有意义。

4.2.3 Kerberos V5 身份验证

Kerberos V5 是域中进行身份验证的重要安全协议。Kerberos V5 协议同时要验证用户的身份和网络服务，这种双重验证称为相互身份验证。

Kerberos V5 身份验证机制颁发用于访问网络服务的票证。这些票证包含加密的数据，其中包括加密的密码，用于向请求的服务确定用户的身份。除了输入密码或智能卡凭据，整个身份验证过程对用户都是不可见的。在每个 Windows Server 2003 域控制器上的 Active



Directory 目录服务中，都有 Kerberos V5 的一个重要服务——密钥发行中心（KDC）在运行，它存储了所有客户端密码和其他账户信息。Kerberos V5 身份验证过程按如下方式进行工作。

（1）客户端系统上的用户使用密码或智能卡向 KDC 进行身份验证。

（2）KDC 为此客户颁发一个特别的票证——授予式票证。客户端系统使用票证（TGT）访问票证授予服务（TGS），这是域控制器上的 Kerberos V5 身份验证机制的一部分。

（3）TGS 接着向客户颁发服务票证。

（4）客户向请求的网络服务出示服务票证。服务票证向此服务证明用户的身份，同时也向该用户证明服务的身份。

Kerberos V5 服务安装在每个域控制器上，并且 Kerberos V5 客户端安装在每个工作站和服务器上。每个域控制器作为 KDC 使用。客户端使用域名服务（DNS）定位最近的可用域控制器。域控制器在用户登录会话中作为该用户的首选 KDC 运行。如果首选 KDC 不可用，系统将定位备用的 KDC 来提供身份验证。

对于在安装过程中所有加入到 Windows Server 2003 域的计算机，都默认启用 Kerberos V5 身份验证协议。Kerberos V5 可对域内的资源和驻留在受信任的域中的资源提供单一登录。

可通过那些作为账户策略一部分的 Kerberos V5 安全设置，来控制 Kerberos V5 配置的某些方面。例如，可设置用户的 Kerberos V5 票证生存周期。作为管理员，可以使用默认的 Kerberos V5 策略，也可以更改它以适应环境的需要。需要注意的是，Kerberos V5 策略不存在于本地计算机策略中，它仅出现在加入到域中的计算机策略安全设置中。

使用 Kerberos V5 进行成功的身份验证，需要两个客户端系统都必须运行 Windows 2000、Windows Server 2003 或 Windows XP Professional 操作系统。如果客户端系统尝试向运行其他操作系统的服务器进行身份验证，则使用 NTLM 协议作为身份验证机制。

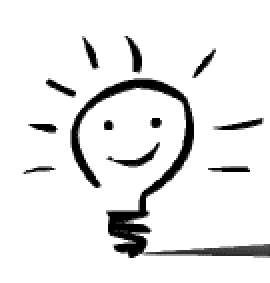
另外，使用 Kerberos V5 进行身份验证的计算机，必须使其时间设置在 5 分钟内与常规时间服务同步，否则身份验证将失败。运行 Windows Server 2003、Windows XP 或 Windows 2000 的计算机将自动更新当前时间，并将域控制器用作网络时间服务。

Kerberos V5 策略主要包含以下方面的内容。

（1）用户登录限制。该安全设置确定 Kerberos V5 密钥分发中心（KDC）是否要根据用户账户的用户权限，来验证每一个会话票证请求。验证每一个会话票证请求是可选的，因为额外的步骤需要花费时间，并可能降低服务的网络访问速度。默认值为已启用。

（2）服务票证最长寿命。该安全设置确定使用所授予的会话票证可访问特定服务的最长时间（以分钟为单位）。该设置必须大于 10 分钟并且小于或等于用户票证最长寿命设置。如果客户端请求服务器连接时出示的会话票证已过期，服务器将返回错误消息。客户端必须从 Kerberos V5 密钥分发中心（KDC）请求新的会话票证。然而一旦连接通过了身份验证，该会话票证是否仍然有效就无关紧要了。会话票证仅用于验证和服务器的新建连接。如果用于验证连接的会话票证在连接时过期，则当前的操作不会中断。默认值为 600 分钟（10 小时）。

（3）用户票证最长寿命。该安全设置确定用户票证授予票证（TGT）的最长使用时间（单位为小时）。用户 TGT 期满后，必须请求新的或“续订”现有的用户票证。默认值为



10 小时。

（4）用户票证续订最长寿命。该安全设置确定可以续订用户票证授予票证（TGT）的期限（以天为单位）。默认值为 7 天。

（5）计算机时钟同步的最大容差。本安全设置确定 Kerberos V5 所允许的客户端时钟和提供 Kerberos V5 身份验证的 Windows Server 2003 域控制器上的时间的最大差值（以分钟为单位）。为防止轮番攻击，Kerberos V5 在其协议定义中使用了时间戳。为使时间戳正常工作，客户端和域控制器的时钟应尽可能地保持同步。因为两台计算机的时钟常常不同步，所以管理员可使用该策略来设置 Kerberos V5 所能接受的客户端时钟和域控制器时钟间的最大差值。如果客户端时钟和域控制器时钟间的差值小于该策略中指定的最大时间差，那么在这两台计算机的会话中使用的任何时间戳都将被认为是可信的。该设置并不是永久性的。如果配置该设置后重新启动计算机，那么该设置将被还原为默认值。默认值为 5 分钟。

如果本地计算机加入到 Windows Server 2003 域中，那么在“组策略编辑器”的“账户策略”中将出现 Kerberos V5 文件夹，管理员可以像设置账户策略一样对 Kerberos V5 的各项参数进行设置。

4.3 用户权限设置

本节所介绍的用户及权限，主要针对的是本地用户及其权限。

本地用户位于独立服务器的计算机管理中，用户可以利用这一组管理工具来管理本地或远程计算机；可以使用本地用户保护并管理存储在本地计算机上的用户账户；可以在特定计算机和仅这台计算机上指派本地用户账户的权限和权利。

通过本地用户，可以为用户和组指派权利和权限，从而限制用户和组执行某些操作的能力。权利可授权用户在计算机上执行某些操作，如备份文件和文件夹或者关机；权限是与对象（通常是文件、文件夹或打印机）相关联的一种规则，它规定哪些用户可以访问该对象以及以何种方式访问。

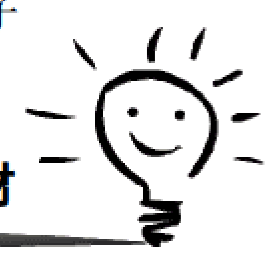
4.3.1 Windows Server 2003 内置账户及组

1. 内置账户

在安装运行 Windows Server 2003 的独立服务器或成员服务器时，系统会自动创建一些默认用户账户，其如下所述。

（1）Administrator 账户。Administrator 账户具有对服务器的完全控制权限，并可以根据需要向用户指派用户权利和访问控制权限。该账户必须仅用于需要管理凭据的任务。强烈建议将此账户设置为使用强密码。

Administrator 账户是服务器上 Administrators 组的成员，且永远也不能从 Administrators 组中删除 Administrator 账户，但可以重命名或禁用该账户。由于大家都知道“管理员”存



在于许多版本的 Windows 上，所以重命名或禁用此账户，将使恶意用户尝试并访问该账户变得更为困难。Administrator 账户是首次设置服务器时使用的账户。在系统使用者为自己创建账户前，应使用该账户进行工作。需要指出，即使已经禁用了 Administrator 账户，仍然可以在安全模式下使用该账户访问计算机。

（2）Guest 账户。Guest 账户由在这台计算机上没有实际账户的用户使用。如果某个用户的账户已被禁用，但还未删除，那么该用户也可以使用 Guest 账户。Guest 账户不需要密码。默认情况下，Guest 账户是禁用的，但也可以启用它。

可以设置 Guest 账户的权利和权限，设置方式与其他用户一样。默认情况下，Guest 账户是默认的 Guests 组的成员，该组允许用户登录服务器。其他权利及任何权限都必须由 Administrators 组的成员授予 Guests 组。默认情况下将禁用 Guest 账户，并且建议将其保持禁用状态。

（3）HelpAssistant 账户（与远程协助会话一起安装）。HelpAssistant 账户用于建立远程会话的主账户。当用户请求远程协助会话时，并且具有对计算机的有限访问权，将自动创建该账户。HelpAssistant 由“远程桌面帮助会话管理器”服务管理，在不存在挂起的远程协助请求时，它会被自动删除。

2. 内置本地组

组是 Windows Server 2003 中对用户账号的一种逻辑单位，将具有相同特点和属性的用户组合成一个组，其目的是方便管理和使用。

如果一个服务器上需要管理很多用户，其中的某些用户具有相同的权限（比如人事部的工作人员账号权限几乎一致），如果单独对每个用户赋予权限，管理维护很不方便，而且十分繁琐。建立组后，对组赋予服务器的权限，只需要将用户加入到该组中，用户将自动具备组的权限。这样管理和维护就十分方便了。

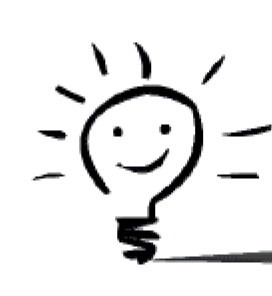
独立服务器上的组又称为本地组。Windows Server 2003 内置的本地组主要包括 Administrators、Backup Operators、Guests、Power Users、Remote Desktop Users、Users 等。

① Administrators 组。该组的成员具有对服务器的完全控制权限，并且可以根据需要向用户指派用户权利和访问控制权限。管理员账户也是默认成员。当该服务器加入域中时，Domain Admins 组会自动添加到该组中。由于该组可以完全控制服务器，所以向该组添加用户时应谨慎。

② Backup Operators 组。该组的成员可以备份和还原服务器上的文件，而不管保护这些文件的权限如何。这是因为执行备份任务的权利要高于所有文件权限，它们不能更改安全设置。

③ Guests 组。该组的成员拥有一个在登录时创建的临时配置文件，在注销时，该配置文件将被删除。来宾账户（默认情况下已禁用）也是该组的默认成员。

④ Power Users 组。该组的成员可以创建用户账户，然后修改并删除所创建的账户。他们可以创建本地组，然后在他们已创建的本地组中添加或删除用户。还可以在 Power Users 组、Users 组和 Guests 组中添加或删除用户。成员可以创建共享资源并管理所创建的



共享资源。他们不能取得文件的所有权、备份或还原目录、加载或卸载设备驱动程序，或者管理安全性以及审核日志。

⑤ Remote Desktop Users 组。该组的成员可以远程登录服务器，允许通过终端服务登录。

⑥ Users 组。该组的成员可以执行一些常见任务，例如运行应用程序、使用本地和网络打印机以及锁定服务器。用户不能共享目录或创建本地打印机。默认情况下，Domain Users、Authenticated Users 及 Interactive 组是该组的成员。因此，在域中创建的任何用户账户都将成为该组的成员。

4.3.2 用户权限设置

用户权限是允许用户在计算机系统或网络中执行任务，用户权限分配则是确定哪些用户或组具有这些权限。

一般情况下，用户权限都是由管理员作为计算机系统或网络的安全设置的一部分，分配给这些计算机或网络的使用者，用户权限可以是针对单个用户进行设置，也可以作为一个组来进行分配。

在 Windows Server 2003 的“组策略编辑器”窗口中，有一个文件夹专门用来对本地用户账号或组进行权限设置，管理员可以在其中根据具体情况进行安全设置。

执行“开始”→“运行”命令，在“打开”文本框中输入 gpedit.msc，单击“确定”按钮，打开如图 4.15 所示的“组策略编辑器”窗口。依次展开“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”→“用户权限分配”文件夹，在其中进行本地用户权限的各种安全设置，如图 4.15 所示。

双击其中的任何一个用户权限设置选项，将出现一个相应内容的对话框，要求操作者选择该权限的拥有者——用户或组，单击“添加用户或组”按钮即可对用户或组进行增加，而选择已有的任何一个用户或组，则可以通过单击“删除”按钮来删除该用户或组，如图 4.16 所示。管理员只需根据当前的用户权限安全策略来进行操作即可。

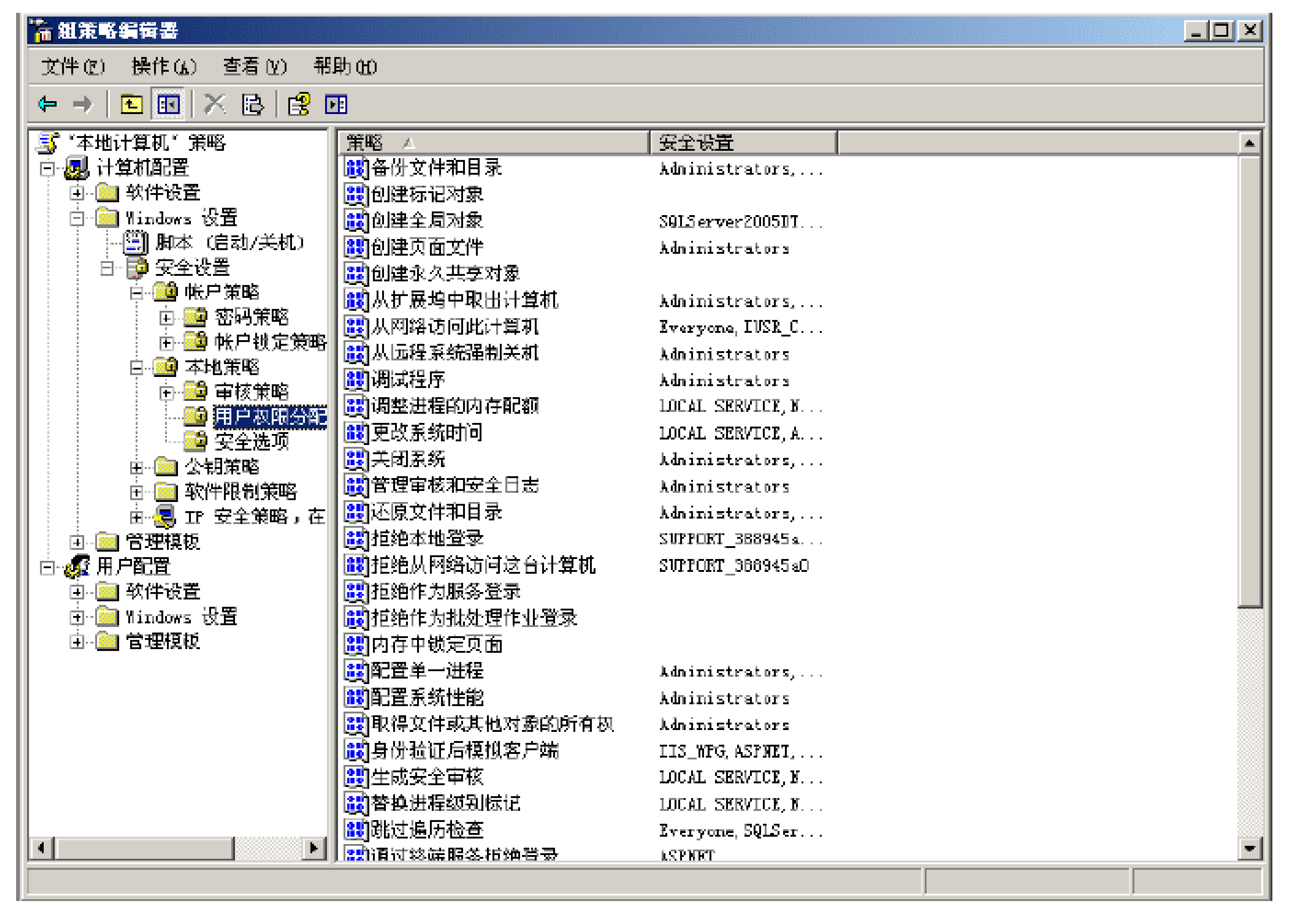


图 4.15 “用户权限分配”文件夹

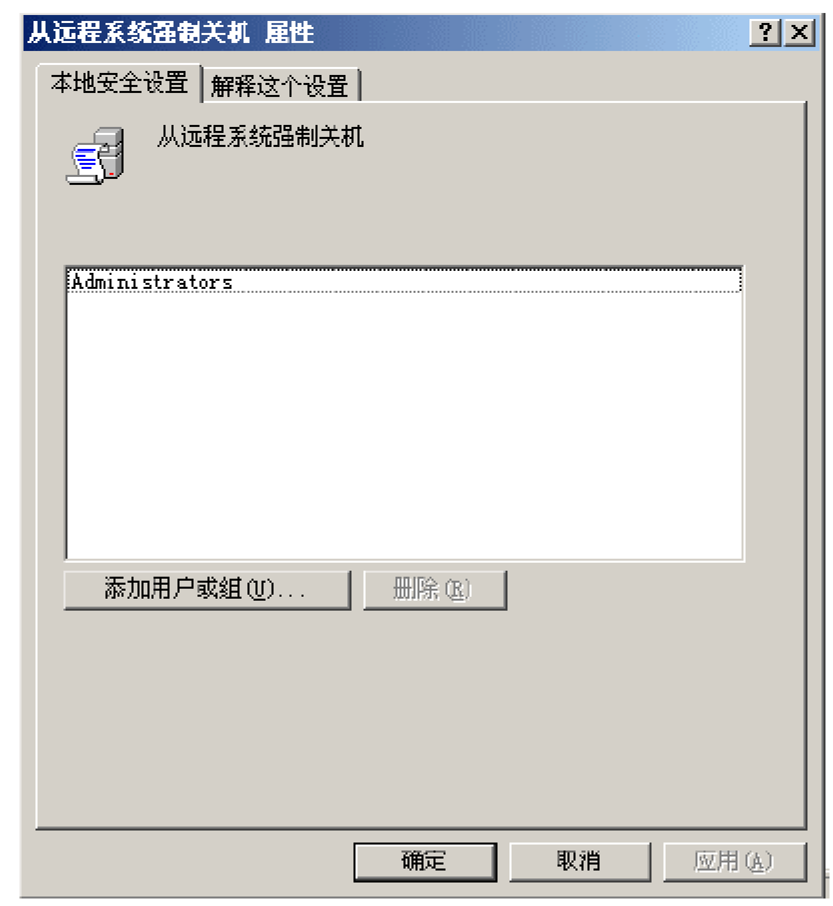


图 4.16 “从远程系统强制关机 属性”对话框



4.4　Windows Server 2003 数字证书

Windows Server 2003 为电子商务提供了一个理想的平台，其安全性包括证书管理、CA（Certification Authority，证书颁发机构）服务、公用密钥基本体系，保证了电子商务的开展。通过 Windows Server 2003 提供的 CA 服务，企业可以为用户颁发各种电子证书，而每个用户或本地计算机上都有自己的一个证书管理器，用来存放和管理自己从 CA 申请获得的证书，也有自己所信任的 CA 的根证书。

4.4.1　证书及证书服务概述

1．证书

证书，通常是用于身份验证及保证公开网络上信息安全性的数字文档。证书将公钥安全地绑定到持有相应私钥的实体中。证书由证书颁发机构（CA）数字签名，并且可以颁发给用户、计算机或服务。接收证书的实体是证书的“主题”。证书的颁发者和签名者是证书颁发机构。通常证书包含以下信息。

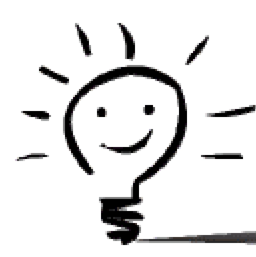
- ☑ 主题的公钥值。
- ☑ 主题标识符信息（如名称和电子邮件地址）。
- ☑ 有效期（证书的有效时间）。
- ☑ 颁发者标识符信息。
- ☑ 颁发者的数字签名，用来证明主体的公钥和主体的标识符信息之间的绑定关系是否有效。

证书只有在指定的期限内才有效，每个证书都包含有效期的起止日期，它们是有效期的界限。一旦到了证书的有效期，到期证书的主题就必须申请一个新的证书。如果在某些情况下必须撤销证书中所声明的绑定关系，这时，可以由颁发者吊销该证书。每个颁发者维护一个证书吊销列表，程序可以使用该列表检查任意给定证书的有效性。

证书的主要好处之一是主机不必再为单个主题维护一套密码，这些单个主题进行访问的先决条件是需要通过身份验证。相反，主机只需在证书颁发者中建立信任。当主机（如安全 Web 服务器）指派某个颁发者为受信任的根证书颁发机构时，主机实际上是信任该颁发者过去常用来建立所颁发证书的绑定关系的策略。事实上，主机信任颁发者已经验证了证书主体的身份。主机通过将包含颁发者公钥的颁发者自签名证书放到主机的受信任根证书颁发机构的证书存储区，将该颁发者指定为受信任的根颁发机构。中间的或从属的证书颁发机构受到信任的条件是它们拥有受信任根证书颁发机构的有效证书路径。

因为证书通常用来为实现安全的信息交换建立身份并创建信任，所以证书颁发机构（CA）可以把证书颁发给人员、设备（例如计算机）和计算机上运行的服务（例如 IPSec）。

某些情况下，计算机必须能够在高度信任涉及交易的其他设备、服务或个人的身份的情况下进行信息交换。某些情况下，人们需要在高度信任涉及交易的其他个人、计算机或



服务的身份的情况下进行信息交换。运行计算机的应用程序和服务也频繁地需要确认它们正在访问的信息来自可信任的信息源。

当两个实体（如设备、个人、应用程序或服务）试图建立身份和信任时，如果两个实体都信任相同的证书颁发机构，就能够在它们之间实现身份和信任的结合。一旦证书主题已呈现由受信任的 CA 所颁发的证书，那么，通过将证书主题的证书存储区存在它自己的证书存储区中，并且（如果适用）使用包含在证书中的公钥来加密会话密钥，以便随后所有与证书主题进行的通信都是安全的，试图建立信任的实体就可以继续进行信息交换。

客户端计算机证书可以服务于多个目的，这些目的大多数是基于身份验证的，这就允许客户端使用很多组织的资源，而不需要为每个资源分别准备证书。例如，客户端证书可能允许 VPN 连接，还允许访问公司 Intranet 站点、产品服务器以及存储雇员数据的人力资源数据库。

很多组织安装有自己的证书颁发机构，并将证书颁发给内部的设备、服务和雇员，以创建更安全的计算环境。大型组织可能有多个证书颁发机构，它们被设置在指向某个根证书颁发机构的分层结构中。这样，雇员的证书存储区中就可能有多个由各种内部证书颁发机构所颁发的证书，而所有这些证书颁发机构均通过到根证书颁发机构的证书路径共享一个信任链接。当雇员利用虚拟专用网（VPN）从家里登录到组织的网络时，VPN 服务器可以提供服务器证书以建立起自己的身份。因为公司的根颁发机构被信任，而公司根证书颁发机构颁发了 VPN 服务器的证书，所以，客户端计算机可以使用该连接，并且雇员知道其计算机实际上连接到组织的 VPN 服务器。在数据可以经过 VPN 连接进行交换之前，VPN 服务器还必须能够验证 VPN 客户端的身份。或者通过交换计算机证书发生计算机级别的身份验证，或者通过使用点对点协议（PPP）身份验证方法，发生用户级别的身份验证。

VPN 服务器证书还可能服务于多个目的。相同证书可能的目的有确认电子邮件服务器、Web 服务器或者应用程序服务器的身份。颁发证书的证书颁发机构决定每个证书的用途数目。

2. 证书服务

证书服务提供了一种可自定义的服务，用以颁发和管理在使用公钥技术的软件安全系统中所用的证书。企业可以通过 Windows Server 2003，使用证书服务来创建证书颁发机构（CA），并通过该颁发机构来负责接收证书申请、验证申请中的信息和申请者的身份、颁发证书、吊销证书以及发布证书吊销列表（CRL）。

在 Windows Server 2003 中，证书服务可用于下列几个方面。

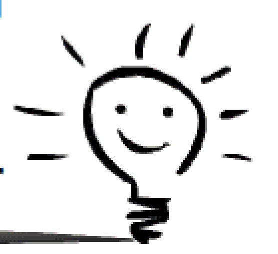
（1）使用 Web 或 Microsoft 管理控制台（MMC）管理单元从 CA 为用户注册证书，或者通过自动注册透明地为用户注册证书。

（2）根据 CA 所使用的策略，使用证书模板帮助简化在申请证书时申请者必须做出的选择。

（3）利用 Active Directory 目录服务，发布信任的根证书，发布已颁发的证书，发布 CRL。

（4）使用智能卡实现登录到 Windows Server 2003 域的能力。

证书服务能正常地对证书进行各种操作，证书策略在其中起到了很重要的作用。所谓



证书策略，就是一组指导或规则，在处理证书申请、颁发证书、吊销证书和发布 CRL 时使用。这些指导是 CA 上的管理策略和配置设置的组合。

在 Windows Server 2003 中安装证书服务时，将 CA 配置为具有默认规则和设置集。这些默认规则和设置集定义 CA 的特定设置，例如 CA 的证书、它的默认颁发行为以及它的密钥恢复代理。该 CA 还可以安装许多预先配置的证书模板，这些模板用来定义证书申请必须拥有哪些信息，以及如何基于该模板处理进入的证书申请。应用 CA 设置和证书模板设置，以及定义的管理准则的组合，就会产生控制 CA 操作的证书策略。

CA 是一种珍贵的资源，应当为其提供高度的保护。应考虑的具体操作包括下列几个方面。

（1）物理保护。由于 CA 代表企业中的高度信任实体，因此应该根据 CA 证书的内在价值保护它们不被篡改。在物理位置上对 CA 服务器进行隔离，服务器放在只允许安全管理员访问的房间，这样可大大减少此类攻击的可能性。

（2）还原。如果出现硬件故障，则 CA 可能会丢失。这可能会引起大量的管理和操作性问题，而且可阻碍现有证书的吊销。证书服务支持使用“备份”来备份 CA，以便能在事后还原。这是整个 CA 管理过程的一个重要内容。

（3）密钥管理。CA 的密钥是其最珍贵的财产，因为私钥提供了认证过程中相互信任的基础。加密硬件设备可提供防篡改的密钥存储，并将加密操作与服务器上运行的其他软件分离，这将减小 CA 密钥被泄露的可能性。证书服务支持其他来源的加密服务提供程序（CSP），但是，Windows 中包含的文档只能使用 Windows 包含的软件 CSP。如果使用其他来源的 CSP，那么应该与供应商确认该 CSP 可与证书服务一同使用。

4.4.2　Windows Server 2003 证书申请

任何一个证书要合法使用就必须先申请，证书申请必须由有权访问与公钥相关联的私钥的用户、计算机或服务产生，该公钥和私钥对将成为证书的一部分。根据系统管理员建立的公钥策略，计算机和服务可以自动申请证书而不受用户干涉。此外，通过使用注册代理证书，管理员还可以申请智能卡用户证书和智能卡证书，以便代表其他用户登录到系统。

在 Windows Server 2003 中，主要有两种明确申请证书的方法。

☑　使用证书申请向导申请证书。

☑　使用 Windows Server 2003 证书服务网页申请证书。

将证书申请提交给 Windows Server 2003 企业证书颁发机构后，该申请将被立即处理，证书申请将或失败或被授予。如果被授予，将颁发证书，并且系统将提示使用者安装证书。在将证书申请提交给 Windows Server 2003 独立证书颁发机构时，申请将被立即处理，或者，在默认情况下，在证书颁发机构管理员批准或拒绝申请之前，该申请将被视为挂起。在申请被挂起的情况下，证书申请者必须使用证书服务网页检查被挂起证书的状态。

下面就以使用证书申请向导申请证书为例，来说明在 Windows Server 2003 中申请证书的步骤。

（1）执行“开始”→“运行”命令，弹出“运行”对话框，在该对话框的“打开”文本框中输入 mmc 命令，打开“控制台 1”窗口，如图 4.6 所示。在该窗口中执行“文件”



→"添加/删除管理单元"命令，弹出如图 4.7 所示的对话框。在该对话框中添加在控制台管理的管理单元，这里需添加证书。单击"添加"按钮，弹出"添加独立管理单元"对话框，在该对话框中单击选中"证书"选项，如图 4.17 所示。单击"添加"按钮，弹出"证书管理单元"对话框，如图 4.18 所示。选中"我的用户账户"单选按钮，单击"完成"按钮关闭该对话框。依次关闭"添加独立管理单元"对话框、"添加/删除管理单元"对话框回到"控制台 1"窗口中，这时可以看到证书管理已经出现在"控制台 1"窗口中。

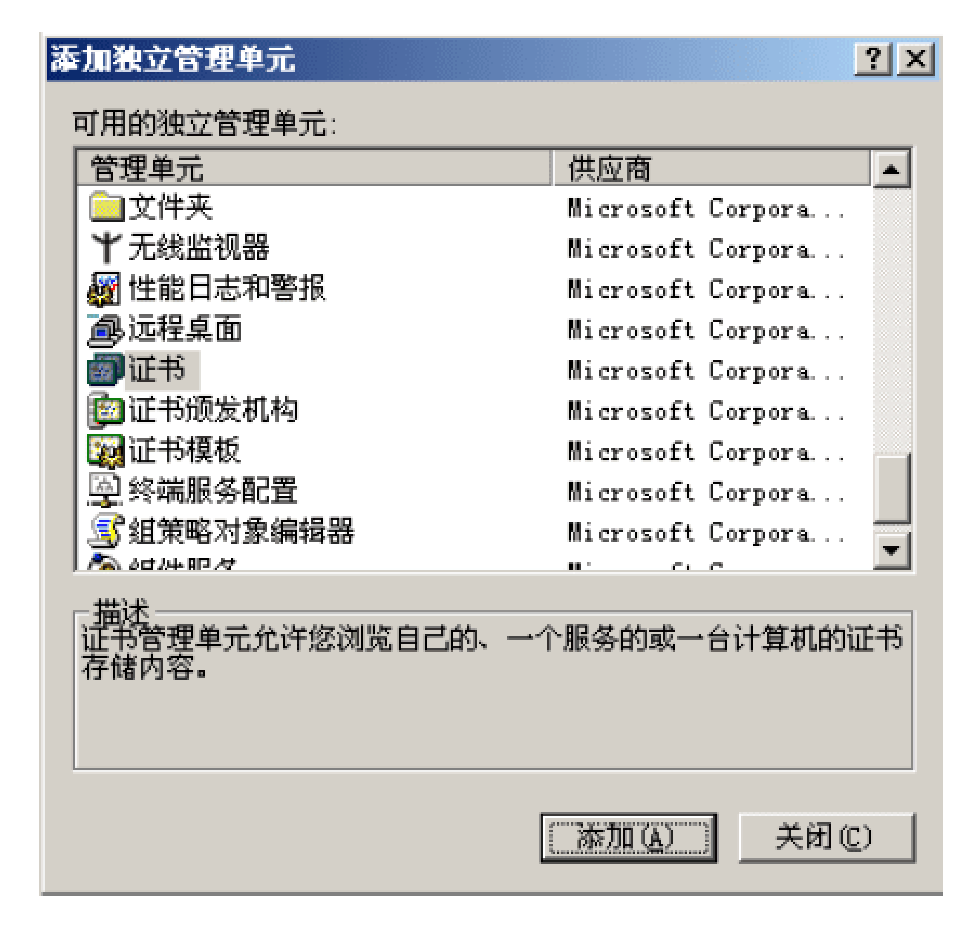


图 4.17　选择"证书"选项

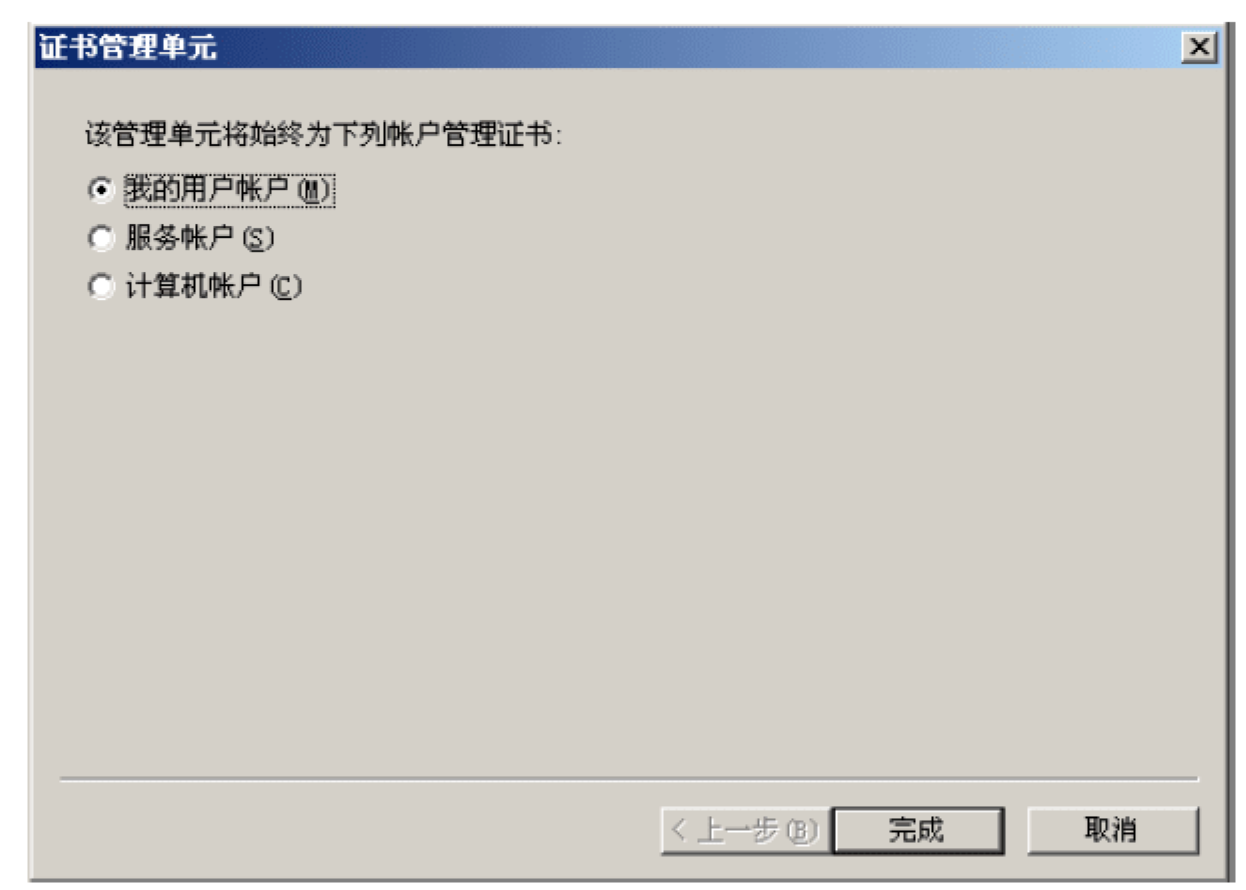


图 4.18　"证书管理单元"对话框

（2）在其中展开"证书-当前用户"文件夹，右击"个人"文件夹，在弹出的快捷菜单中执行"所有任务"→"申请新证书"命令，以启动证书申请向导。

（3）根据证书申请向导中的提示，完成各种参数的输入及选择，最后完成证书申请。需要注意的是，在证书申请向导中，在选择"要申请的证书的类型"时选中"高级"复选框，可以进行下列几项设置。

① 可以选择需设置要使用的加密服务提供程序（CSP）。

② 可以选择需设置与证书关联的公钥钥长（以位为单位）。

③ 如果申请者希望启用强私钥保护，可以选中"启用强私钥保护"复选框。启用强私钥保护将确保在每次使用私钥时都有提示信息。

④ 如果申请者具有多个可用的证书颁发机构（CA），可以选择将颁发证书的证书颁发机构的名称。

4.4.3　Windows Server 2003 证书信任的管理

证书申请完成并通过 Windows Server 2003 系统的 CA 授予后，就可以在网络中正式使用了。但证书是有使用时间限制的，或者证书的密钥发生了变化，这些都需要管理员或证书使用者及时地对证书进行更新。

Windows Server 2003 提供有 3 种证书管理方式，通过它们能够方便、及时地更新证书。

（1）自动更新受信任根颁发机构。

使用安全网站或收发安全电子邮件时，一般使用证书。从理论上来说，任何人都可以



颁发证书，但是为了实现可靠的安全交易，必须由受信任的实体或组织来颁发证书。在 Windows Server 2003 中包含了一个它视为受信任的颁发机构的公司和组织的列表。

一般而言，当使用者遇到浏览器或操作系统提供的受信任颁发机构列表以外的颁发机构颁发的证书时，系统会询问是否在颁发证书的证书颁发机构（CA）中建立信任。需要注意的是，许多用户都不愿意以这种方式建立对于颁发机构的信任，因为他们用仅有的有限资源来验证该 CA 的可信度和颁发策略。

在 Windows Server 2003 中，可以使用“更新根证书”功能实现该任务。默认情况下，“更新根证书”处于启动状态。启动该项功能，当使用者遇到由不信任的根颁发机构颁发的证书时，计算机将联系 Windows Update 网站，查看 Microsoft 是否已将该 CA 添加到其受信任的颁发机构列表中。如果已经添加，则证书将自动添加到受信任证书存储区中。

（2）管理第三方证书颁发机构的信任。

默认情况下，安装 Windows Server 2003 时，大量证书颁发机构（CA）颁发的证书，将列在第三方根证书颁发机构物理存储区中。第三方根证书颁发机构存储区包含了使用者的组织以外的公司的受信任的根证书颁发机构（CA）。管理员可在“组策略”中选择“仅信任的根证书颁发机构”选项，来禁用这些 CA 的信任。用户访问第三方根证书颁发机构没有验证的任何安全网站时，他们将收到安全警告，通知他们不信任这些站点。

（3）管理用户选定的证书颁发机构的信任。

对于使用者来说，所有信任的根证书都存储在“受信任的根证书颁发机构”下。管理员可使用“组策略”来禁用使用者选定的根证书颁发机构（CA）的信任。网络用户访问这些使用者选定的根证书颁发机构未验证的任何安全网站时，他们将收到安全警报警告，通知他们不信任这些站点。

4.5　使用审核资源

审核功能用于跟踪用户访问资源的行为与 Windows Server 2003 的活动情况，这些行为或活动称为事件，会被记录到日志文件内，利用“事件查看器”可以查看这些被记录的审核数据。建立审核事件是安全的重要内容之一。通过监控对象的创建和修改可以追踪潜在的安全问题，有助于确保用户账户的可用性，并为指证破坏安全的事件提供依据。

4.5.1　审核事件

在 Windows Server 2003 中，可以被审核并记录在安全日志中的事件类型有以下几种。

- ☑ 审核策略更改。
- ☑ 审核登录事件。
- ☑ 审核对象访问。
- ☑ 审核过程追踪。
- ☑ 审核目录服务访问。



- ☑ 审核特权使用。
- ☑ 审核系统事件。
- ☑ 审核账户登录事件。
- ☑ 审核账户管理。

4.5.2 事件查看器

当 Windows Server 2003 系统出现有误（如网卡故障）、用户登录/注销的行为或者应用程序发出错误信息等情况时，Windows Server 2003 会将这些事件记录到事件日志文件内，可以利用“事件查看器”来检查这些日志，看看到底发生了什么，以便做进一步的处理工作。

Windows Server 2003 的事件日志文件分为以下 4 大类。

（1）系统日志。Windows 2000 会主动将系统所产生的错误（如显示故障）、警告（如 CPU 的利用率太高）与系统信息（如某个服务已被启动了）等信息记录到系统日志内。

（2）安全日志。它会记录“审核策略”所设置的事件发生情况，例如某个用户是否曾经读取过某一个文件。

（3）应用程序日志。它是由应用程序所产生的错误、警告或信息等事件记录到此日志文件内。例如若数据库程序有误时，它可以将此错误记录到应用程序日志内。

（4）目录服务日志。它会记录由 Active Directory 所发出的诊断或错误信息。这个日志只存在于域控制器内。

1. 查看事件记录

可以通过以下两种方法来启动“事件查看器”。

（1）执行“我的电脑”→“管理”→“系统工具”→“事件查看器”命令。

（2）执行“开始”→“程序”→“管理工具”→“事件查看器”命令。

打开“事件查看器”窗口，如图 4.19 所示，其右边窗格是“系统”日志文件的记录信息，图中每一行代表一个事件，它提供了以下信息。

（1）类型：此事件的类型，如错误、警告、信息等。

（2）日期与时间：此事件被记录的日期与时间。

（3）来源：记录此事件的程序名称。

（4）分类：产生此事件的程序可能会将其信息分类，此分类信息会被显示在“分类”列中。

（5）事件：每个事件都会被赋予一个唯一的号码，这个号码显示在这个“事件”列中。

（6）用户：当事件发生时，正在使用此计算机的用户，或者制造此事件的用户。

（7）计算机：发生此事件的计算机名称。

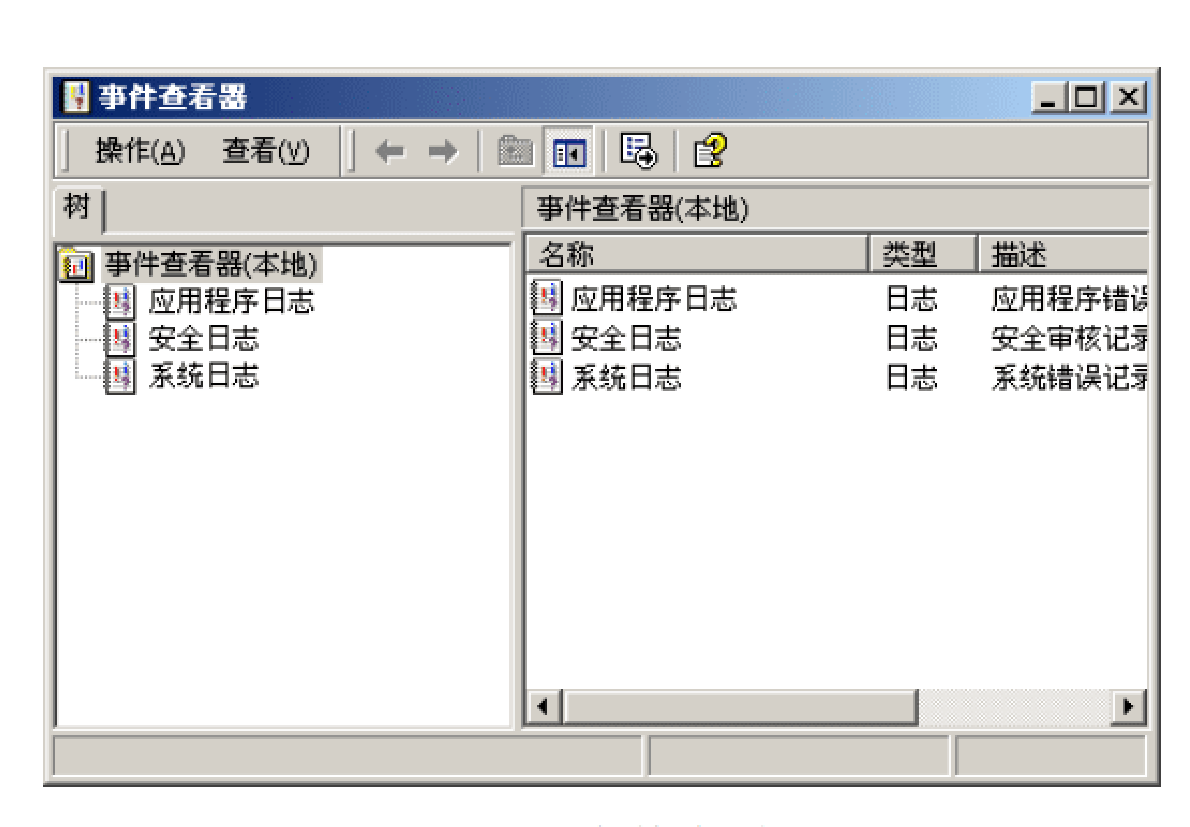
若要查看事件的详细信息，请直接双击该事件或右击该事件并选择“属性”命令，将出现如图 4.20 所示的对话框。

如果要清除某个日志（系统、安全、应用程序等）内的所有事件，则只要右击该日志文件并选择“清除所有事件”命令或在图 4.21 中单击“清除日志”按钮即可。



2. 设置日志文件的大小

可以针对每个日志文件（系统、安全、应用程序等）来更改其设置，例如，日志文件容量的大小等。设置时请选中该日志文件名，单击鼠标右键，在弹出的快捷菜单中选择“属性”→“常规”命令，将出现如图 4.21 所示的对话框。



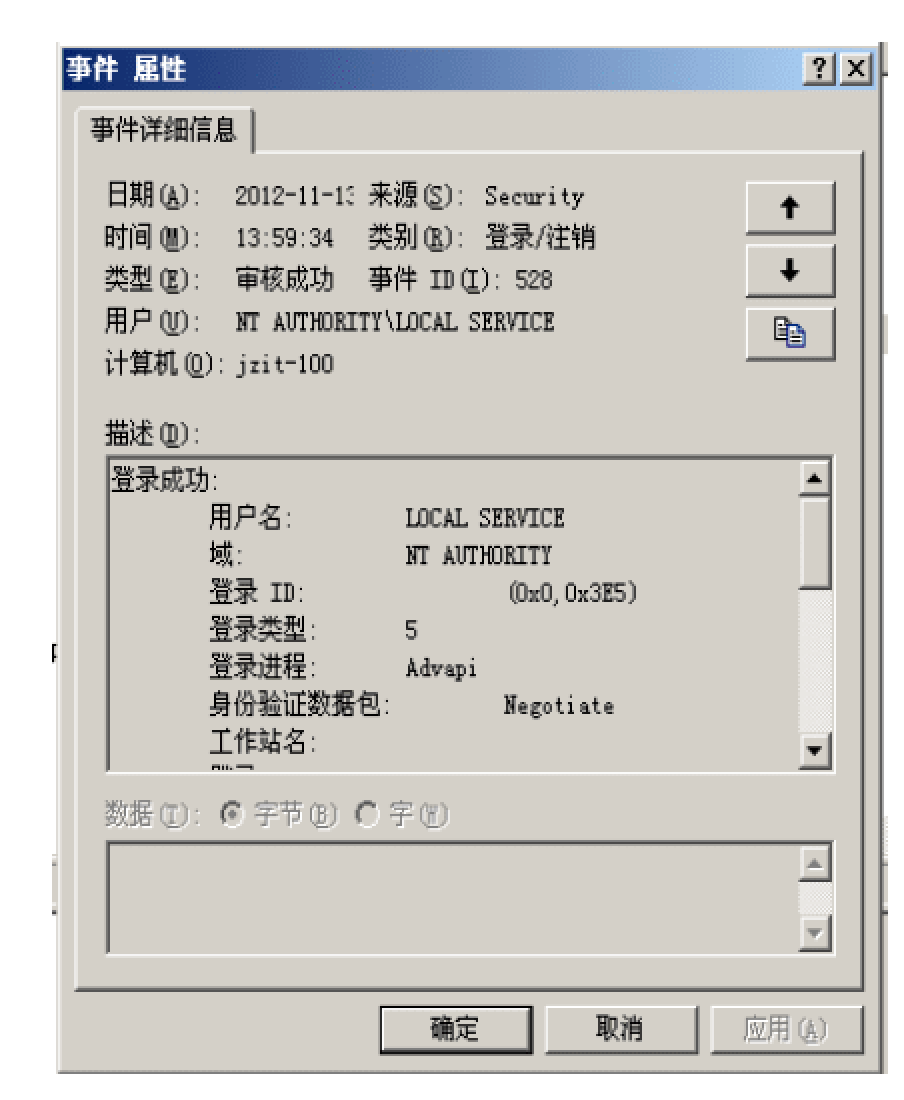



图 4.19　事件查看器　　　　图 4.20　事件的详细信息

（1）最大日志文件大小：用来设置该日志文件的大小，默认为 512KB，可以增加或减少其值，不过日志文件的大小必须是 64KB 的倍数。

（2）当达到最大的日志尺寸时：用来设置当日志文件满载时，应该如何记录新的事件。

☑ 按需要改写事件：继续记录新的事件，但是会将旧的事件覆盖掉。

☑ 改写久于××天的事件：会将××天前的旧事件覆盖掉，以便继续记录新的事件。

☑ 改写事件：不会继续记录新的事件，此时必须以手动方式清除日志文件。

（3）清除日志：将此日志文件清除，如果需要的话，可以在清除之前先将此数据存盘（通过右击该日志文件并选择“另存日志文件”命令进行保存）。

3. 筛选事件日志中的事件

如果日志文件内的事件太多，造成不易查找事件时，可以利用筛选事件的方式，让它只显示特定的事件。该设置可通过右击该日志文件名并选择“属性”→“筛选器”命令，或者右击该日志文件名并选择“查看”→“筛选”命令的途径实现，将出现如图 4.22 所示的对话框，从中可以根据事件的类型、事件来源、类别、计算机、事件发生的起始/结束时间等设置选择要显示的事件。

若要取消筛选功能，则可以通过右击该日志文件名并选择“查看”→“所有记录”命令的途径实现。

4. 存储日志文件的格式

存储日志文件的格式可以是以下 3 种形式。

（1）事件日志。其扩展名为.evt，是“事件查看器”查看的默认日志格式。



（2）文本（以制表符分隔）。其扩展名为.txt，是将每一条数据之间利用制表符（Tab）分隔。以此格式存储的文件，可利用一般的文字处理软件（如记事本等）查看，也可供电子表格、数据库等应用程序来读取、导入。

（3）CSV（以逗号分隔）。其扩展名为.csv，它是将每一条数据之间用逗号“,”分隔。以此格式存储的文件，可利用一般的文字处理软件（如记事本等）来查看，也可供电子表格、数据库等应用程序来读取、导入。

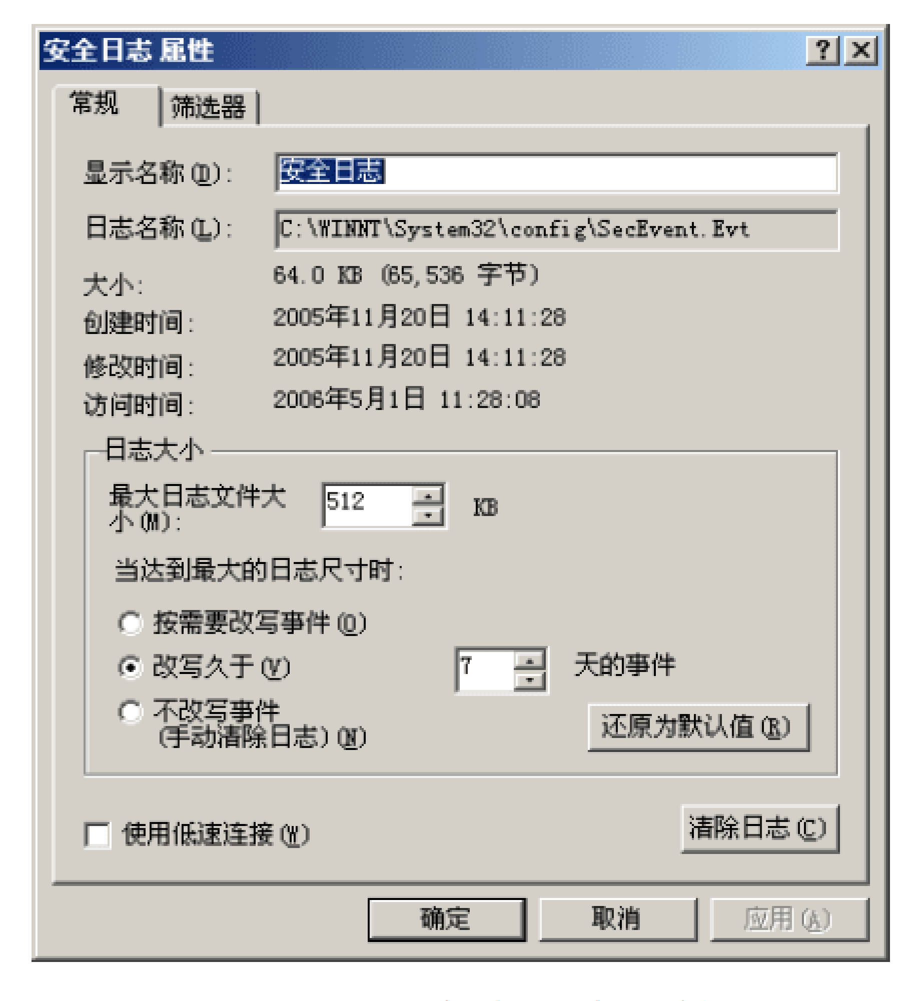


图 4.21　安全日志属性

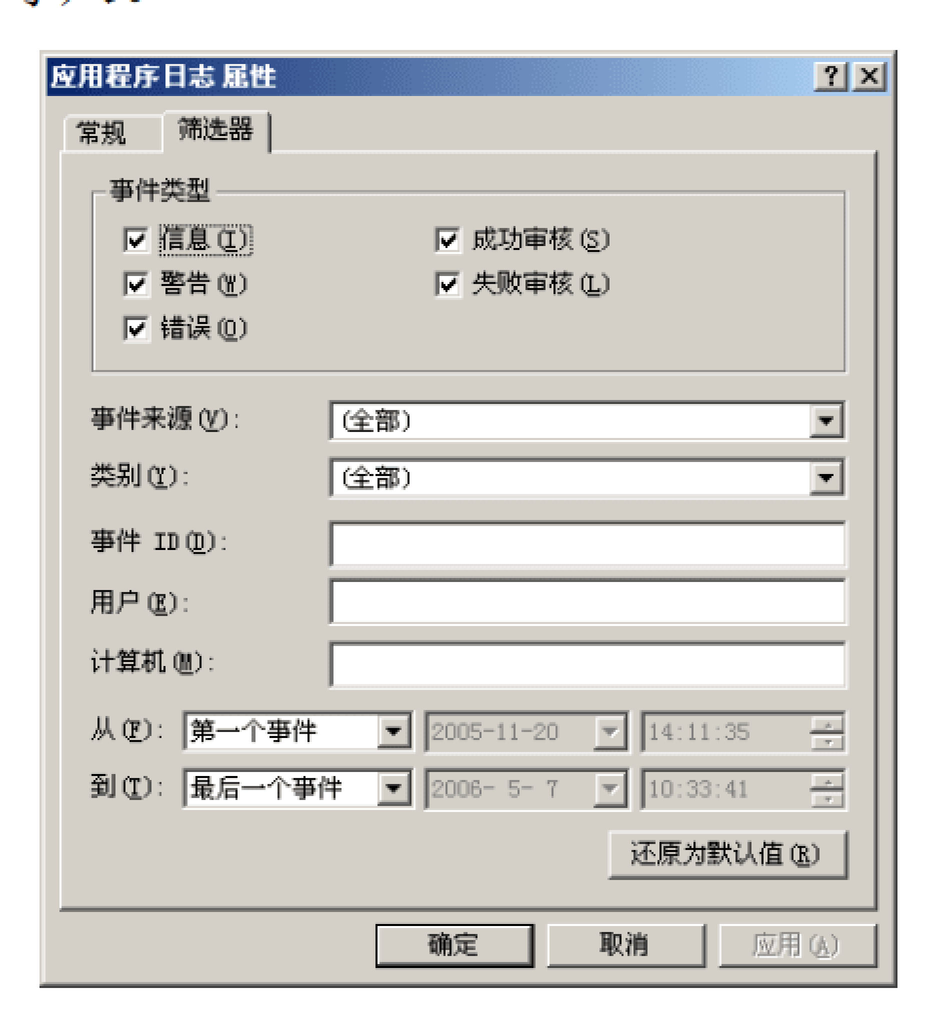


图 4.22　筛选事件日志中的事件

4.5.3　使用审核资源

1. 制定审核策略

审核策略用于设置是否对系统一些重要事件进行审核。制定事件的审核时需要综合考虑，如果审核太多的事件会造成系统开销太大，审核太少的事件有可能不能保证系统的安全。主要应考虑与系统安全性密切相关的事件。

具体来说，制定审核策略时应主要考虑以下问题。

（1）确定要审核的事件类型。

① 访问网络资源，如文件、文件夹或打印机等。

② 用户登录和注销。

③ 关闭和重新启动运行 Windows Server 2003 的计算机。

④ 修改用户账户和组。

（2）确定审核成功的事件与审核失败的事件或者两者都审核。

① 账户管理：成功、失败。

② 登录事件：成功、失败。

③ 对象访问：失败。

④ 策略更改：成功、失败。

⑤ 特权使用：失败。

⑥ 系统事件：成功、失败。

⑦ 目录服务访问：失败。

⑧ 账户登录事件：成功、失败。

（3）确定查看安全日志的时间表。

要审核用户访问资源的情况，必须经过以下两个步骤。

① 设置审核策略。条件是只有具备 Administrator 权限的用户才能设置审核策略。

② 设置要审核的资源。必须具备“管理审核及安全日志”权限的用户才可以审核资源的使用情况，默认是只有 Administrators 组内的成员才有此权限。可以利用组策略内的“用户权利指派”策略给予其他用户这个权限。如果要审核文件或文件夹的使用情况，则这些文件与文件夹必须位于 NTFS 磁盘分区内，FAT16/FAT32 并不支持审核的功能。另外，最好是将事件日志归档，便于以后查询。

按照审核策略所记录的数据记录在“安全日志”内，可利用“事件查看器”查看此日志。

2. 审核策略的设置

审核策略的设置是通过“组策略”或“本地安全策略”进行的。根据目前正在使用的计算机与设置的对象决定使用“组策略”或“本地安全策略”。另外，如果在本地计算机、站点、域与组织单位内都分别设置了审核策略，则这些审核策略的应用顺序如下。

（1）本地审核策略（通过“本地安全策略”设置）。

（2）站点的审核策略。

（3）域的审核策略。

（4）组织单位（OU）的审核策略。

审核策略应用的总原则是：应用顺序在后的审核策略会覆盖掉应用顺序在前的审核策略，例如，若域的审核策略与本地审核策略的设置有冲突时，则以应用顺序在后的域审核策略内的设置为其最终设置。

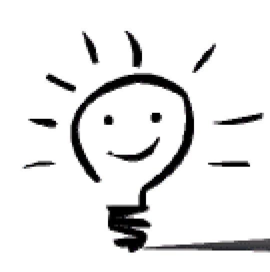
4.6　Windows Server 2003 的安全应用

Windows Server 2003 是微软公司在 Windows 2000 系列的基础上改进推出的，它集成了功能强大的应用程序环境，具有更广泛的适应性和便捷的管理。

对于网络系统管理员来说，最关心的事情莫过于系统的安全。Windows Server 2003 作为 Micorsoft 最新推出的服务器操作系统，相比 Windows 2000/XP 系统来说，各方面的功能确实得到了增强，尤其在安全性方面。但任何事物都不是十全十美的，Windows Server 2003 也存在着系统漏洞和安全隐患。无论用计算机欣赏音乐、上网冲浪、运行游戏，还是编写文档都不可避免地受到新病毒和恶意软件的威胁，如何让 Windows Server 2003 更加安全，就成为广大用户十分关注的问题。

4.6.1　Windows Server 2003 安全

Windows Server 2003 系统不仅继承了 Windows 2000/XP 的易用性和稳定性，而且还提



供了更高的硬件支持和更加强大的安全功能，无疑是中小型网络应用服务器的首选。Windows Server 2003 系统提供的提高密码的破解难度、启用账户锁定策略、限制用户登录、限制外部连接、系统审核机制、监视开放端口和连接、监视进程和系统信息等安全策略，可确保网络安全和服务器的正常运行。

1. 提高密码的破解难度

在 Windows Server 2003 系统中，可以通过在安全策略中设定“密码策略”来提高密码的破解难度。Windows Server 2003 系统的安全策略可以根据网络的情况，针对不同的场合和范围进行有针对性的设定。例如可以针对本地计算机、域及相应的组织单元进行设定，这将取决于该策略要影响的范围。以域安全策略为例，其作用范围是网中所指定域的所有成员。在域管理工具中运行“域安全策略”工具，就可以针对密码策略进行相应的设定。密码策略也可以在指定的计算机上用本地安全策略来设定，同时也可在网络中特定的组织单元通过组策略进行设定。

2. 启用账户锁定策略

Windows Server 2003 系统的账户锁定是指定某些情况下（如账户受到采用密码词典或暴力猜解方式的攻击），为保护该账户的安全而将此账户进行锁定，使其在一定的时间内不能再次使用。默认情况下并没有设定这种锁定策略，用户可根据情况自行设置账户锁定。设定账户锁定的第一次登录尝试，如果 3 次登录全部失败，系统就会锁定该账户。一旦该账户被锁定后，即使合法用户也无法使用了，只有管理员才能重新启用该账户。为方便用户，可以同时设定锁定的时间，这样从开始锁定账户时进行计时，当锁定时间超过该时间后系统自动解锁。虽然这会给用户的使用造成一些不便，但它可以有效地避免自动猜解工具的攻击。设置指定账户锁定的阈值，即确定该账户无效登录的次数。一般设定该数值为 3，即允许 3 次。

3. 限制用户登录

用户还可以通过对其登录行为进行限制，来保障其账户的安全。这样即使是密码出现泄露，系统也可以在一定程度上阻止黑客入侵。Windows Server 2003 网络用户可运行“Active Directory 用户和计算机”管理工具，选择相应的用户并设置其账户属性。在“账户属性”设置中可对其登录时间和地点进行限制。另外，还可以通过“账户”选项限制登录时的行为，如使用“用户必须用智能卡登录”就可避免直接使用密码验证。此外，还可以引入指纹验证等更为严格的手段。

4. 限制外部连接

对于企业网络来说，通常需要为一些远程拨号用户（业务人员或客户）提供拨号接入服务。远程拨号访问技术实际上是通过低速拨号连接将远程计算机接入到企业内部网中。由于该连接无法隐藏，因此常常成为黑客入侵企业内部网的最佳入口，但采取一定的措施可以有效地降低此风险。基于 Windows Server 2003 的远程访问服务器，默认情况下将允许具有拨入权限的所有用户建立连接。因此，合理地设置用户账户的拨入权限，严格限制拨入权限的分配范围，即可很好地限制外部连接。在 Windows Server 2003 系统中，如果活

动目录工作在 Native-mode（本机模式）下，就可以通过存储在访问服务器上或 Internet 验证服务器上的远程访问策略来管理。

5. 限制特权组成员

Windows Server 2003 系统还有一种非常有效的防范黑客入侵和管理疏忽的辅助手段，这就是利用“受限制的组”安全策略。该策略可保证组成员是固定的。在域安全策略的管理工具中添加要限制的组，在“组”对话框中输入或查找要添加的组，然后配置该受限制的组成员，当安全策略生效后，可防止黑客将后门账户添加到该组中。

6. 启用系统审核机制

系统审核机制可以对系统中的各类事件进行跟踪记录并写入日志文件，以供管理员进行分析、查找系统和应用程序故障以及各类安全事件。对 Windows Server 2003 系统的服务器和工作站系统来说，为了不影响系统性能，默认的安全策略并不对安全事件进行审核。从“安全配置和分析”工具用 SecEdit 安全模板进行的分析结果可见，这些有特殊标记的审核策略应该已经启用，这可用来发现来自外部和内部的黑客的入侵行为。对于关键的应用服务器和文件服务器来说，应同时启用共同的安全策略。如果已经启用了“审核对象访问”策略，那么就要求必须使用 NTFS 文件系统。NTFS 文件系统不仅提供对用户的访问控制，而且还可以对用户的访问操作进行审核。但这种审核功能需要针对具体的对象来进行相应的配置。

在被审核对象“安全”属性的“高级”属性中添加要审核的用户和组。在该对话框中选择要审核的用户后，就可以设置对其进行审核的事件和结果。在所有的审核策略生效后，就可以通过检查系统的日志来发现黑客的蛛丝马迹。

7. 监视开放的端口和连接

在系统中启用安全审核策略后，管理员应经常查看安全日志记录，否则就失去了及时补救和防御的时机。对日志的监视只能发现已经发生的入侵事件，对正进行的入侵和破坏行为却无能为力。这时，就需要管理员来掌握一些基本的实时监视技术。

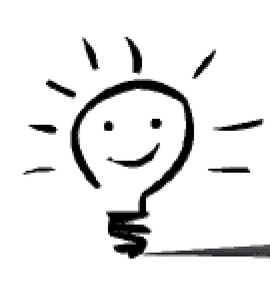
黑客或病毒入侵系统后通常会在系统中留下后门，同时会与外界建立一个 Socket 会话连接进行通信，这时利用 netstat 命令进行会话状态的检查就可能发现已经打开的端口和已经建立的连接。当然可以采用一些专用的检测程序对端口和连接进行检测。

8. 监视共享

黑客通过共享入侵系统是很方便的，最简单的就是利用系统隐含的管理共享。因些，只要黑客能扫描到用户的 IP 和密码，就可使用 netuse 命令连接到共享上，另外，当发现含有恶意脚本的网页时，此时计算机硬盘也就可能被共享，因此，监测本机的共享连接是非常重要的。监测本机的共享连接的具体方法为：在 Windows Server 2003 系统的计算机中，打开“计算机管理”窗口，并展开“共享文件夹”选项，单击其中的“共享”按钮就可以在其窗口中检查是否有新的可疑共享。如果有可疑共享，就应该立即删除。另外还可以通过选择“会话”选项，来查看连接到机器上所有共享的会话。

9. 监视进程和系统信息

对于木马和远程监控程序，除了监视开放的端口外，还应通过任务管理器的进程查看



功能查看进程，在安装 Windows Server 2003 系统支持工具后就可以获得一个进程查看工具 Process Viewer。隐藏的进程通常寄宿在其他进程下，因此查看进程的内存映像也许能发现异常。有些木马会把自己注册成一个服务，从而可避免在进程列表中现形，因此人们还应该加强对系统中其他信息的监视，对系统信息中的软件环境下的各项进行相应的检查。

4.6.2 Windows Server 2003 的安全设置

下面介绍一些 Windows Server 2003 系统常用的安全操作和设置。

1. 清除默认共享隐患

Windows Server 2003 系统在默认安装时，会产生默认的共享文件夹。虽然用户并没有设置共享，但每个盘符都被 Windows 自动设置了共享，其共享名为盘符后面加一个符号$(共享名为 c$、d$、ipc$等)，这样一来，只要攻击者知道了该系统的管理员密码，就有可能通过输入“\\工作站\点共享名\共享名称”来打开系统的指定文件夹，用户精心设置的安全防范就不安全了。因此应将 Windows Server 2003 系统默认的共享隐患从系统中清除掉。可采用以下步骤：

（1）选择“开始”→“运行”命令，输入 gpedit.msc，确认后即可打开“组策略编辑器”窗口。

（2）依次展开“用户配置”→“Windows 设置”→“脚本（登录/注销）”文件夹，如图 4.23 所示。

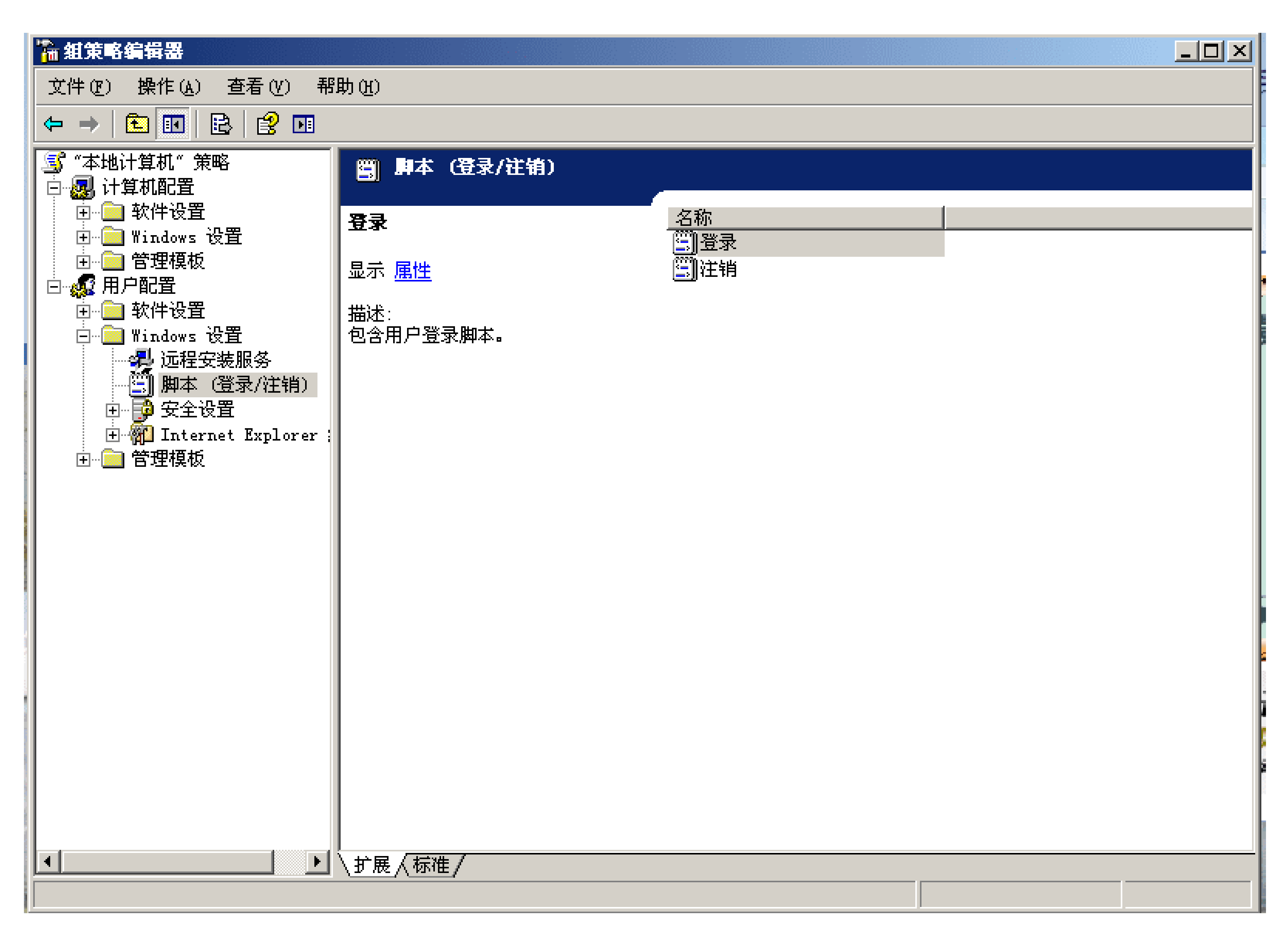
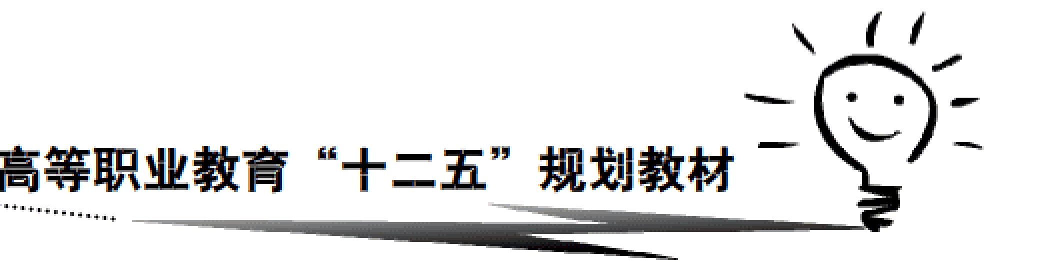


图 4.23 “组策略编辑器”窗口

（3）双击“登录”选项，在出现的“登录 属性”对话框中单击“添加”按钮。

（4）在出现的“添加脚本”对话框的“脚本名”文本框中输入 delshare.bat，然后单击“确定”按钮即可，如图 4.24 所示。



（5）重新启动计算机系统。

这样就可以自动将系统所有的隐藏共享文件夹全部取消，将系统安全隐患降到最低限度。

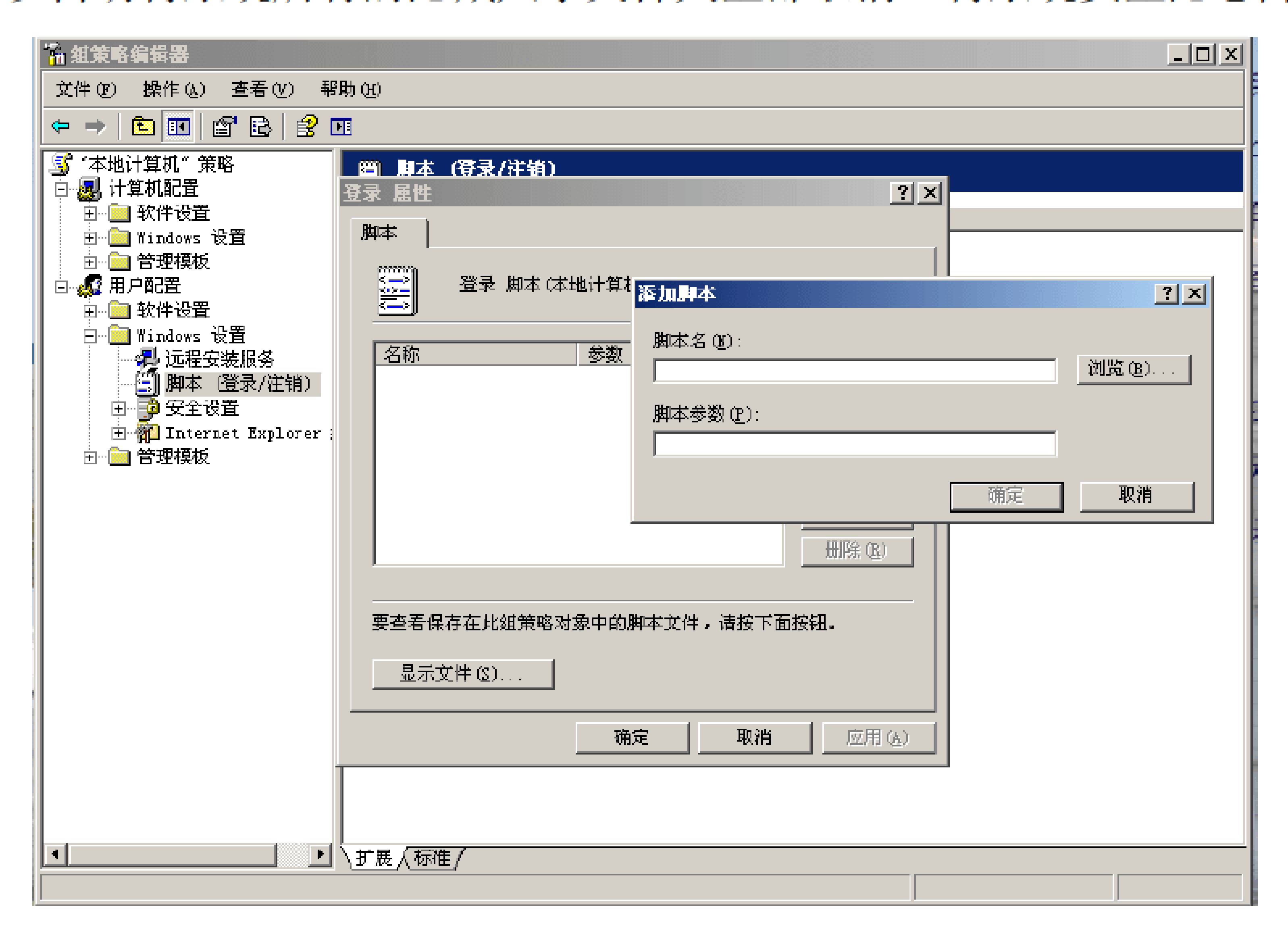


图 4.24 清除默认共享

2. 禁止非法访问应用程序

Windows Server 2003 是一种服务器操作系统。为了防止非法用户登录到系统中并随意启动服务器中的应用程序，给服务器的正常运行带来不必要的麻烦，可根据不同用户的访问权限，来限制他们去调用应用程序。实际上我们只要使用“组策略编辑器”作进一步的设置，即可实现这一目的。具体步骤如下：

（1）打开“组策略编辑器”窗口，然后依次展开“用户配置”→“管理模板”→“系统”文件夹，如图 4.25 所示。

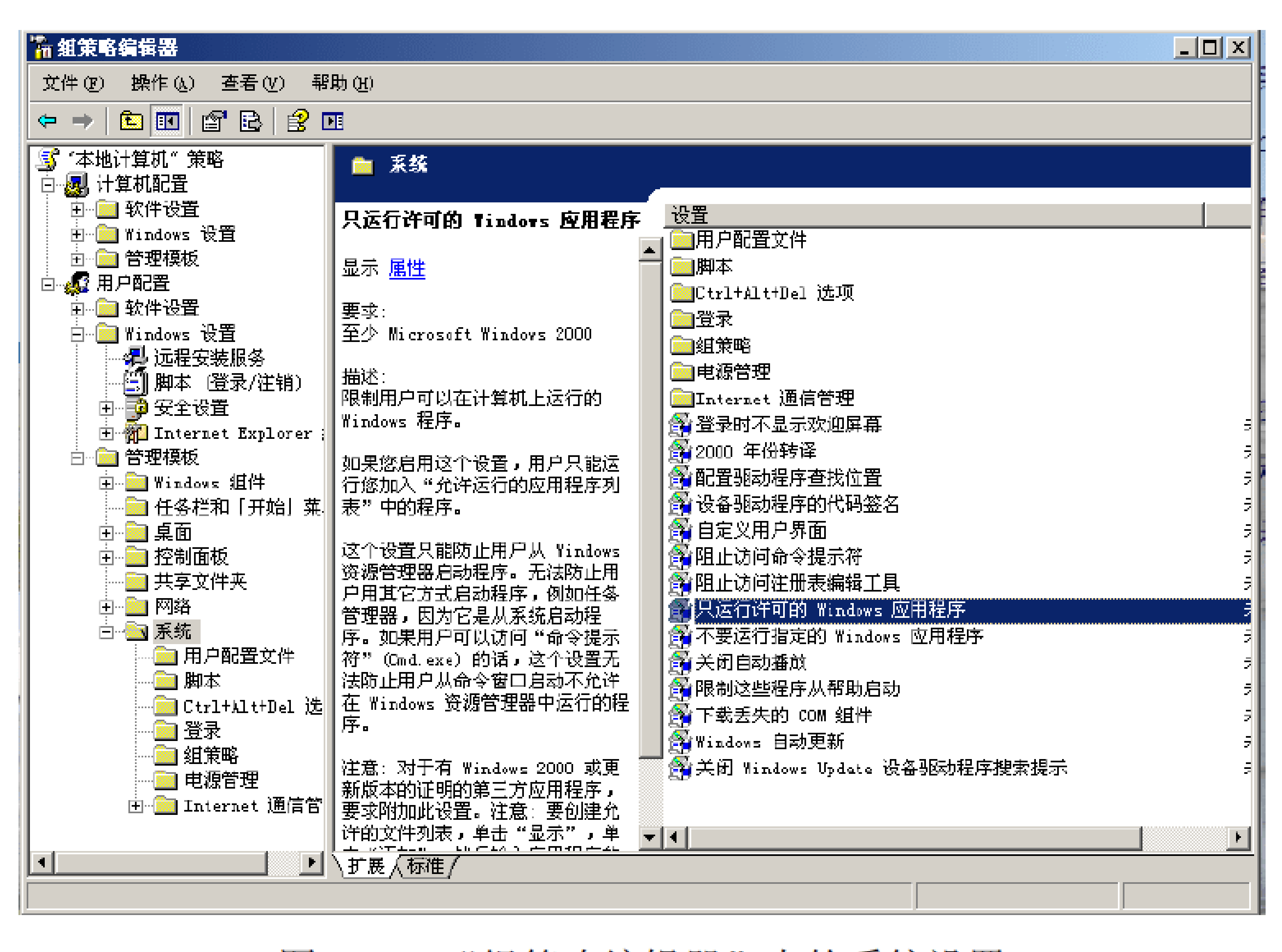


图 4.25 “组策略编辑器”中的系统设置

（2）在“设置”列表框中选择“只运行许可的 Windows 应用程序”选项并双击，在打开对话框的“设置”选项卡中选中“已启用”单选按钮，如图 4.26 所示。

（3）单击“允许的应用程序列表”右边的“显示”按钮，弹出“显示内容”对话框，如图 4.27 所示。

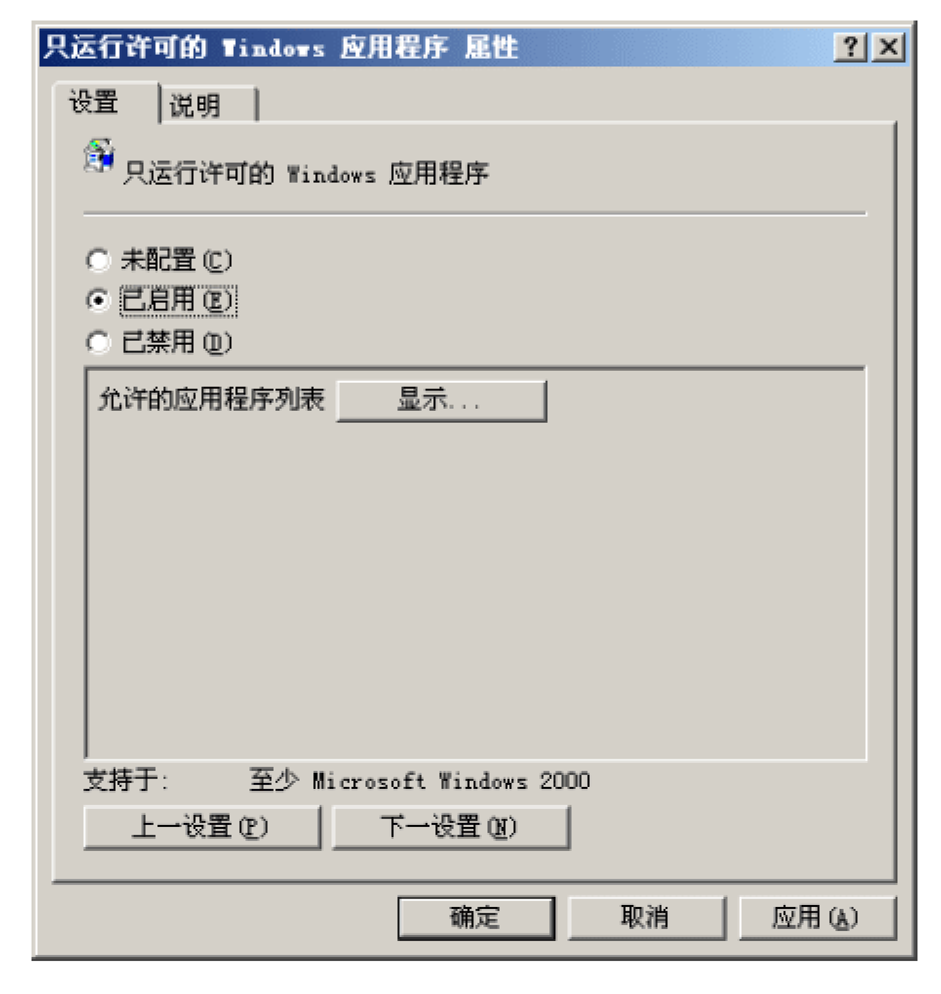


图 4.26 选中“已启用”单选按钮

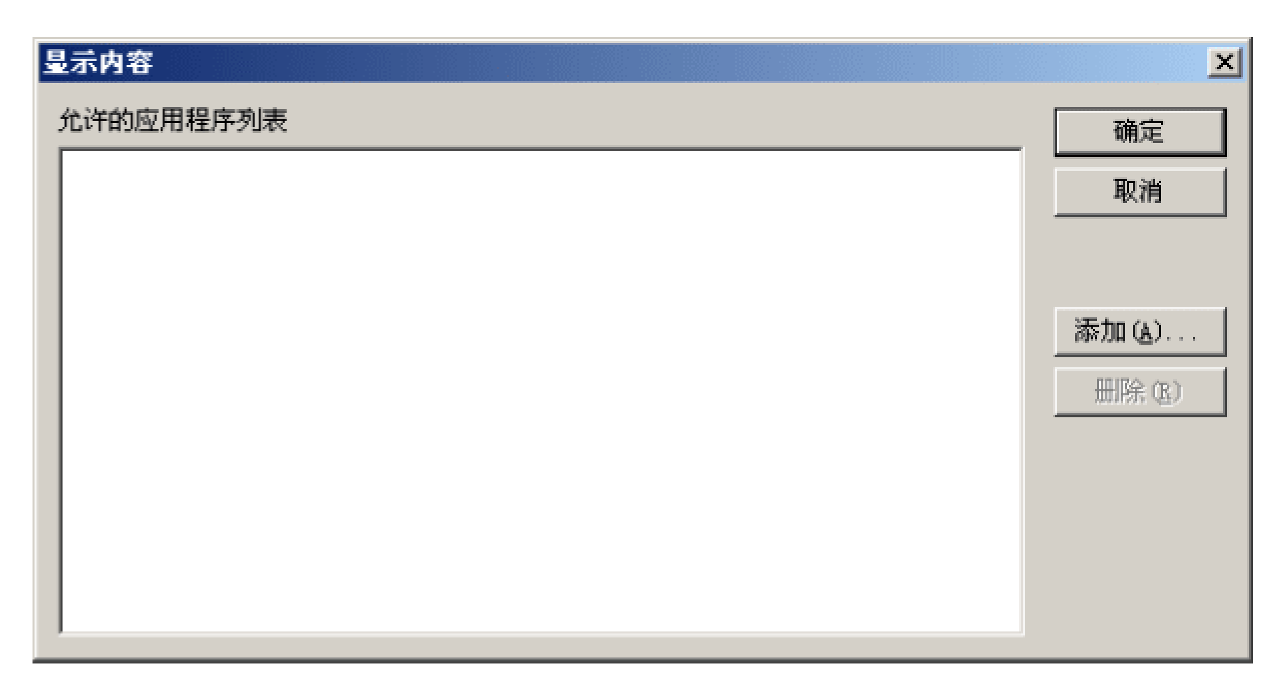


图 4.27 “显示内容”对话框

（4）单击“添加”按钮来添加允许运行的应用程序，如图 4.28 所示。

这样操作后一般用户只能运行“允许的应用程序列表”中的程序。

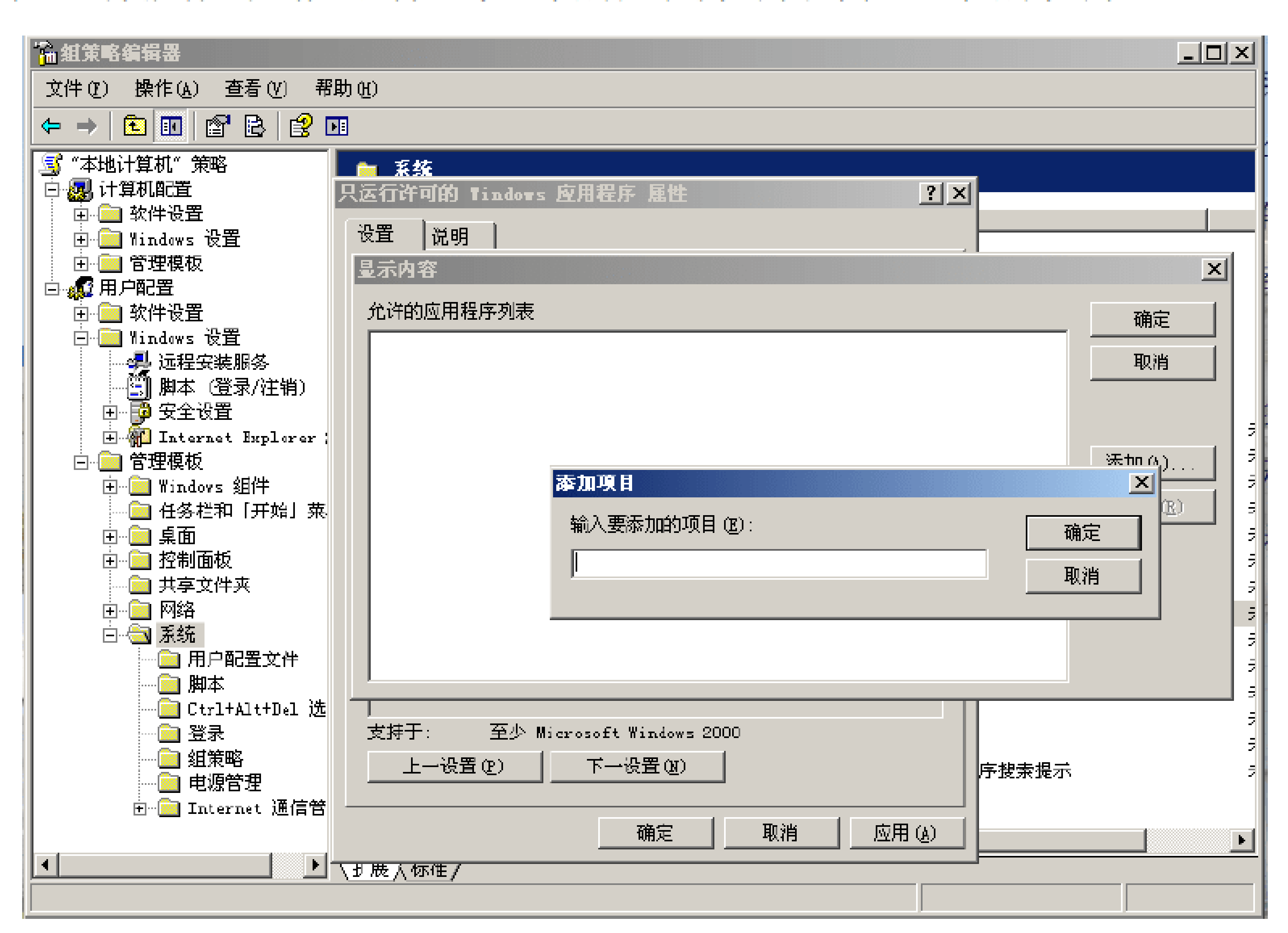


图 4.28 “添加项目”对话框

3. 禁用 IPC 连接

IPC$（Interner Process Connection）是共享命名管道的资源，它是为了使进程间通信而开放的命名管理。通过提供可信任的用户名和口令，连接双方计算机即可建立安全的通道，并以此通道进行加密数据的交换，从而实现对远程计算机的访问。它是 Windows



NT/2000/2003 特有的功能。但它有一个特点，即在同一时间内，两个 IP 之间只允许建立一个连接。系统在提供了 IPC$功能的同时，在初次安装系统时还打开了默认共享，即所有的逻辑共享（c$、d$、e$等）和系统目录 windows（admin$）共享。这虽然为系统管理员的管理提供方便，但也为 IPC 入侵者提供了方便条件，导致系统的安全性能降低，因此，为了安全起见，禁用 IPC 连接。可以通过修改注册表来实现禁用 IPC 连接。

4. 清空远程可访问的注册表路径

Windows Server 2003 系统提供了注册表的远程访问功能，只有将远程可访问的注册表路径设置为空，才能有效地防止黑客利用扫描通过远程注册表读取计算机的系统信息。设置远程可访问的注册表路径为空的步骤如下：

（1）打开“组策略编辑器”窗口，然后依次展开“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”文件夹。

（2）单击“安全选项”选项，双击右侧窗口中的“网络访问：可远程访问的注册表路径”选项。

（3）在打开的“网络访问：可远程访问的注册表路径 属性”对话框中，将可远程访问的注册表路径和子路径内容全部设置为空，再单击“确定”按钮即可，如图 4.29 如示。

另外，在进行安全设置时，对如图 4.29 所示的本地策略的安全选项设置可以考虑将“网络访问：可匿名访问的共享”、“网络访问：可匿名访问的命名管道”和“网络访问：可远程访问的注册表路径和子路径”3 项全部删除；将“网络访问：不允许 SAM 账户的匿名枚举”、“网络访问：不允许 SAM 账户和共享的匿名枚举”、“网络访问：不允许存储网络身份验证的凭据或.NETPassports”和“网络访问：限制匿名访问命名管道和共享”4 项更改为“已启用”。

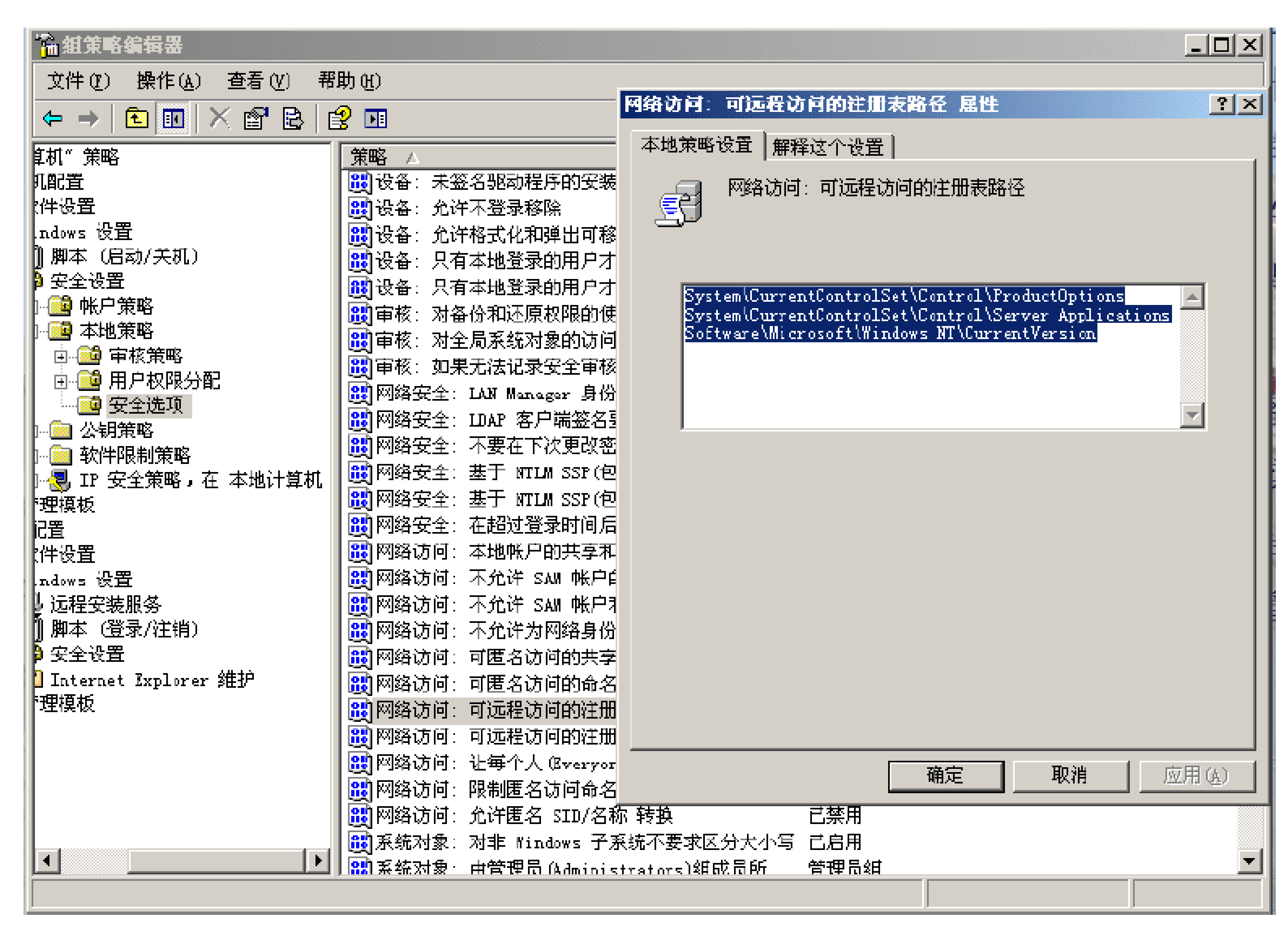
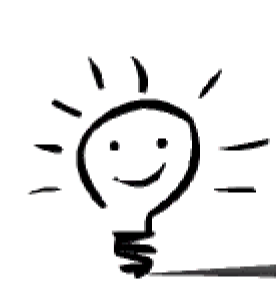


图 4.29 “网络访问：可远程访问的注册表路径 属性”对话框

5. 关闭不必要的端口和服务

对于个人用户来说，系统安装过程中默认的有些端口没有什么用途，应该关掉这些端



口，即关闭无用的服务。

（1）关闭 139 端口。

139 端口是 NetBIOS 协议所使用的会话服务端口，在安装了 TCP/IP 协议的同时，NetBIOS 也会被作为默认设置安装到系统中。该端口的开放意味着硬盘可能会在网络中共享，网上黑客可通过 NetBIOS 了解用户计算机中的一切。在以前的 Windows 版本中，只要不安装“Microsoft 网络的文件和打印机共享”协议，就可关闭 139 端口。但在 Windows Server 2003 系统中，要单独进行关闭 139 端口的操作才行。具体步骤如下：

① 右击“网络邻居”，在弹出的快捷菜单中选择“属性”命令，进入“网络 连接”窗口。

② 右击“本地连接”，在弹出的快捷菜单中选择“属性”命令，打开“本地连接 属性”对话框。

③ 取消选中“Microsoft 网络的文件和打印机共享”复选框，如图 4.30 所示。

④ 选中“Internet 协议（TCP/IP）”复选框，单击“属性”按钮，在打开的对话框中再单击“高级”按钮，打开“高级 TCP/IP 设置”对话框，选择 WINS 选项卡，选中“禁用 TCP/IP 上的 NetBIOS”单选按钮，单击“确定”按钮即可完成任务，如图 4.31 所示。

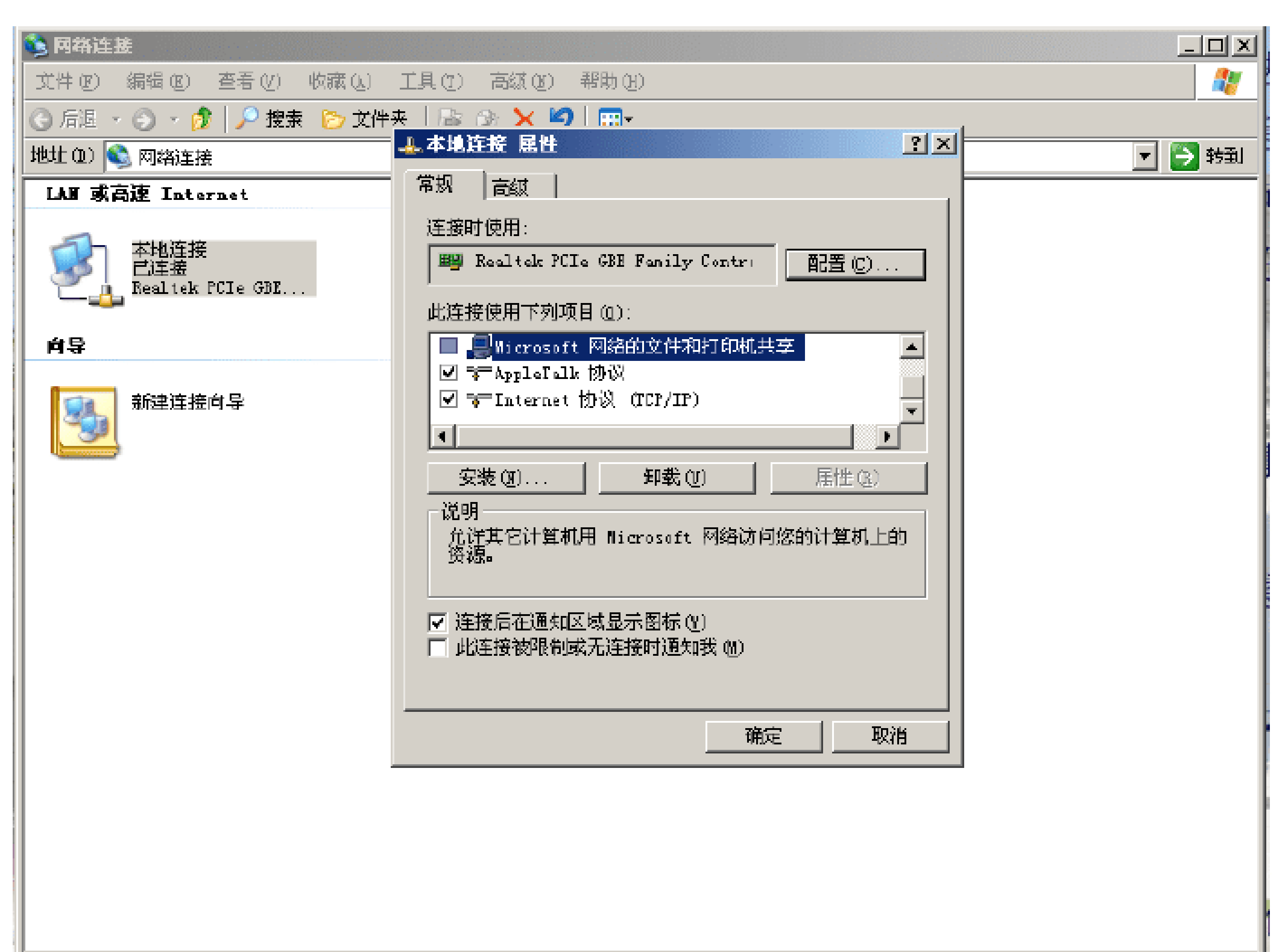


图 4.30 “本地连接 属性”对话框

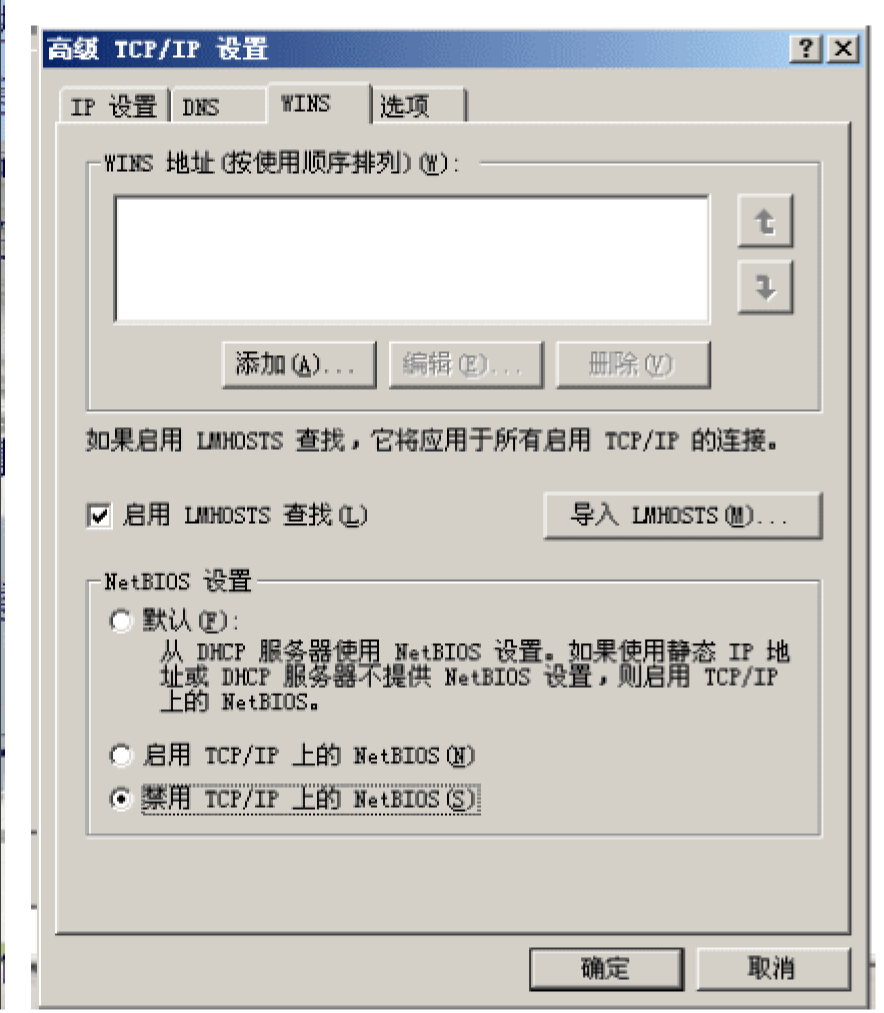


图 4.31 禁用 TCP/IP 上的 NetBIOS

（2）关闭 445 端口。

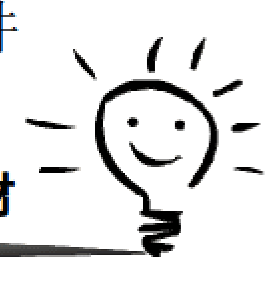
445 端口是一把“双刃剑”，有了它用户可以在局域网中轻松访问各种共享文件夹或共享打印机，但也正是因为有了它，黑客们才有了可乘之机。他们可通过该端口偷偷共享用户的硬盘，甚至会在悄无声息中将用户的硬盘格式化。用户要做的就是想办法不让黑客有机可乘，封堵住 445 端口漏洞。关闭 445 端口的方法是，打开注册表后做如下操作：

选择 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NetBT\Parameters 中的 Parameters 选项并右击，在弹出的快捷菜单中选择“新建”→“DWORD 值”命令，将 DWORD 值命名为 SMBDeviceEnabled，数值为 0。

（3）关闭 135 端口。

关闭 135 端口的步骤如下：

① 执行“开始”→“运行”命令，输入 dcomcnfg，单击“确定”按钮，打开“组件



服务”对话框。

② 在“组件服务”对话框中展开“组件服务”→“计算机”文件夹，如图 4.32 所示。在“计算机”文件夹中，右击“我的电脑”，在弹出的快捷菜单中选择“属性”命令。

③ 在弹出的“我的电脑 属性”对话框的“默认属性”选项卡中，取消选中“在此计算机上启用分布式 COM”复选框，如图 4.33 所示。

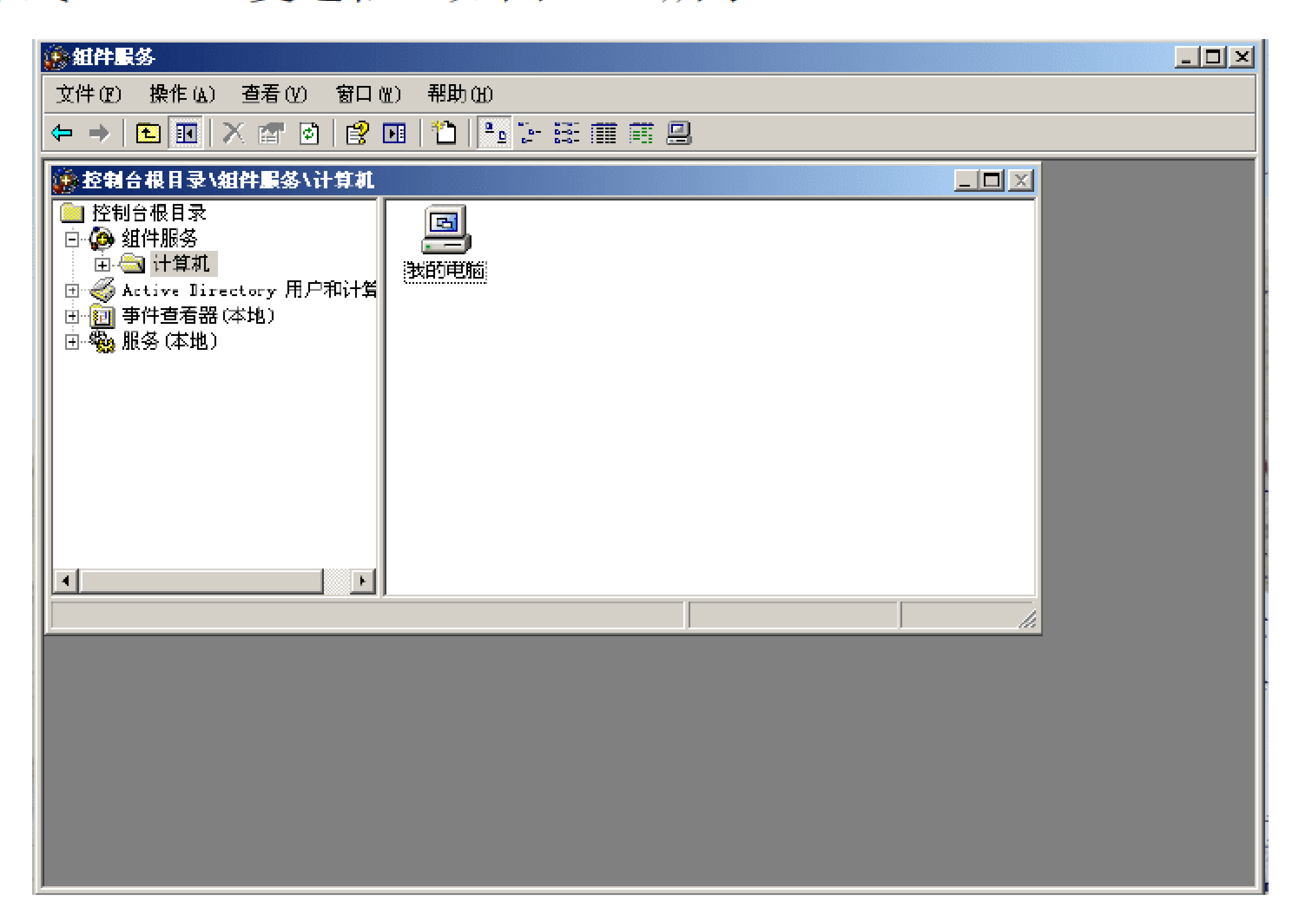


图 4.32　“组件服务”对话框

④ 选择“默认协议”选项卡，选择“面向连接的 TCP/IP”选项，单击“移除”按钮。再单击“确定”按钮完成设置，如图 4.34 所示。

重新启动计算机后即可关闭 135 端口。

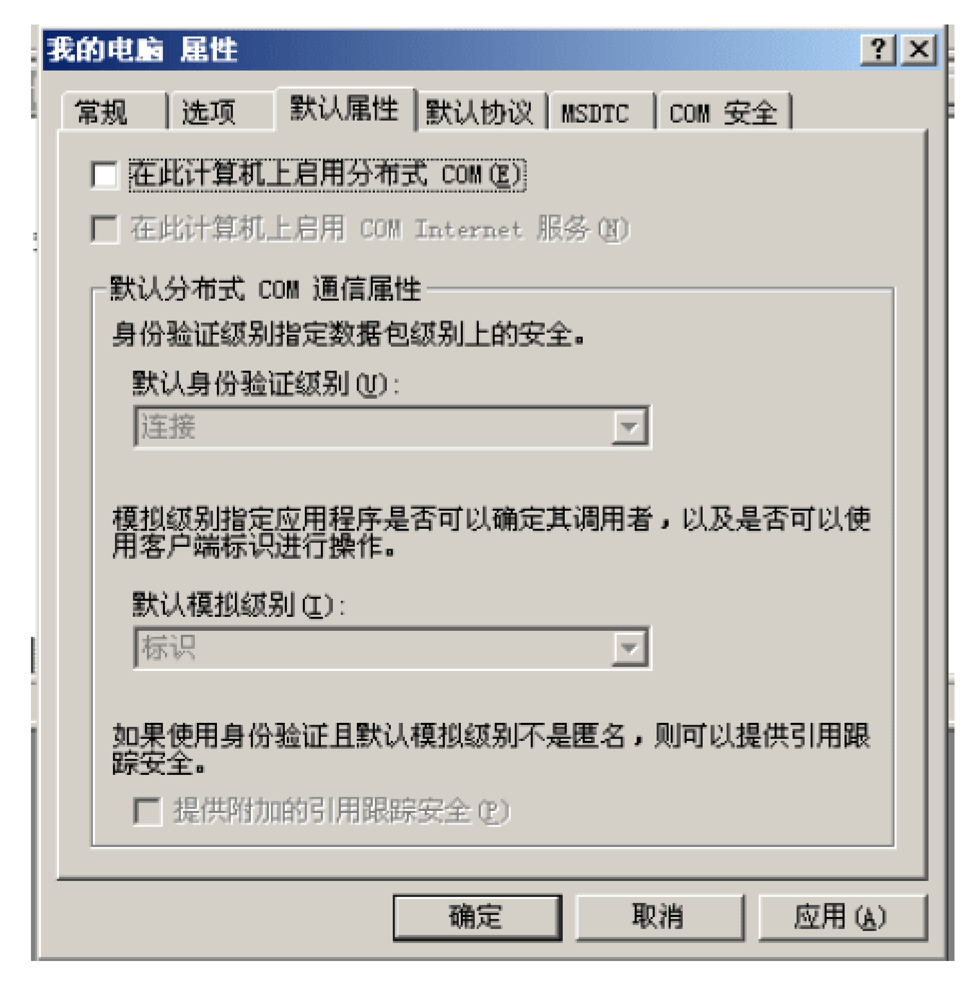


图 4.33　“我的电脑 属性”对话框



图 4.34　面向连接的 TCP/IP

（4）关闭自动播放等服务。

自动播放功能不仅对光驱起作用，而且对其他驱动也起作用。自动播放功能很容易被黑客利用来执行黑客程序，因此，可以考虑关闭该服务。关闭自动播放服务的操作为：

① 打开“组策略编辑器”窗口，依次展开“计算机配置→管理模板→系统”文件夹。



② 在右侧窗口中找到“关闭自动播放”选项并双击。

③ 在打开的对话框中选中“已启用”单选按钮，然后在“关闭自动播放”后面的下拉列表框中选择“所有驱动器”选项，单击“确定”按钮即可生效。

另外，打开“本地连接”的 Windows Server 2003 自带的防火墙，可以屏蔽端口，基本可达到 IPSec（Internet 协议安全性）的功能。例如，只保留远程桌面服务器端口 3389、Web 服务器端口 80、FTP 服务器端口 21、邮件服务器端口 25、POP3 服务器端口 110、网页浏览端口 443 和 SQL 监听端口 1433 等有用的端口，将其余端口屏蔽掉。

把不必要的服务都禁止掉，尽管这些不一定能被攻击者利用得上，但是按照安全规则和标准看，多余的东西就没有必要开启，这样还可减少一份隐患。对于个人用户，可以在各项服务属性设置中将要关闭的服务设为“禁用”，这样在下次重启服务后不需要的服务就关闭了。

Windows Server 2003 系统中还可以关闭如下不常用的服务。

① Computer Browser（维护网络上计算机的最新列表及提供这个列表）。

② Task scheduler（允许程序在指定时间运行）。

③ Messager（传输客户端和服务器之间的 NET SEND 和警报器服务消息）。

④ Distributed File System（分布式文件系统）。

⑤ Distributed linktracking client（用于局域网更新连接信息）。

⑥ Error Reporting Service（发送错误报告）。

⑦ Microsoft Search（提供快速的单词搜索）。

⑧ PrintSpooler（如果没有打印机可禁用）。

⑨ Remote Registry（远程修改注册表）。

⑩ Remote Desktop Help Session Manager（远程协助）。

6. 删除不安全的组件

一些 ASP 木马或一些恶意程序都会使用到 WScript.Shellt 和 Shell.application 这两个组件，采用如下方法可删除或卸载这两个组件。

（1）通过注册表删除。删除注册表 HKEY_CLASSES_ROOT\CLSID\{72C24DD5-D70A-438B-8A42-98424B88AFB8}]对应的 WScript.Shell；删除注册表[HKEY_CLASSES_ROOT\CLSID\{13709620-C279-11CE-A49E-444553540000}]对应的 Shell.application。

（2）利用 regsvr32/u 来卸载。利用 regsvr32/u wshom.ocx 卸载 WScript.Shell 组件；利用 regsvr32/u shell32.dll 卸载 Shell.application 组件。

7. 账户锁定设置

账户锁定策略是一项 Active Directory 安全功能。在指定时间段内，如果登录尝试失败次数达到指定次数，它会锁定用户账户并禁止登录。允许尝试的次数和时间段基于为账户锁定设置的值。账户锁定策略还可以指定锁定期限。账户锁定设置有助于防止攻击者猜测用户密码，并且会降低对网络环境攻击成功的可能性。

执行“开始”→“运行”命令，输入 secpol.msc，打开“本地安全设置”窗口，打开“账户锁定策略”文件夹，如图 4.35 所示。双击“账户锁定阈值”选项，在出现的对话框



中输入允许尝试的最大登录次数，单击“确认”按钮即可。

图 4.35　“本地安全设置”窗口

本 章 小 结

本章主要讲述了 Windows Server 2003 新增加的安全功能，Windows Server 2003 中的用户管理及其策略，Windows Server 2003 中的文件访问权限及其策略，Windows Server 2003 中的资源审核、基本应用及在 Windows Server 2003 中安全使用数字证书等内容。

习　　题

一、填空题

1．Active Directory 存储有关网络上________的信息，并让用户和网络管理员可以使用这些信息。

2．Windows Server 2003 系统的身份验证使用对所有网络资源的________登录。

3．访问控制是批准________、组和________________访问网络上的对象的过程。

4．证书通常是用于________及保证公开网络上________________的数字文档。

5．Windows Server 2003 的事件日志文件分为__________、__________、__________、________ 4 大类。

二、选择题

1．在 Windows Server 2003 系统中代表一个用户、组或计算机的符号是________。

A．AT　　B．SAD　　C．ACL　　D．SID

2．在 Windows Server 2003 系统中怎样改变一个本地账户密码________。

A．在用户管理中，右击账户　　B．在本地安全中，右击账户

C．在本地安全策略中，右击账户　　D．在本地用户和组中，右击账户

3．为了设置基于用户的本地文件权限，必须采用________文件系统。

A．FAT　　B．NTFS　　C．UID　　D．GID

4．没有启用 NTFS 之前，下面________功能不能用。

A．日志　　B．删除文件　　C．审核　　D．建立用户共享

5．在 Windows Server 2003 系统事件查看器中，6007 号事件意味着________。

A．一次不成功的登录　　B．关机事件

C．一个不正当的关闭事件　　D．一个错误的服务

本 章 实 训

实训　Windows Server 2003 策略与用户权限配置

实训目的

掌握 Windows Server 2003 操作系统有关策略配置、用户权限配置的相关概念和操作方法。

实训环境

安装了 Windows Server 2003 操作系统的服务器。

操作步骤

1．Windows Server 2003 策略配置

第 1 步：执行“开始”→“运行”命令，在“打开”文本框中输入 gpedit.msc 命令，打开“组策略编辑器”窗口，如图 4.36 所示。

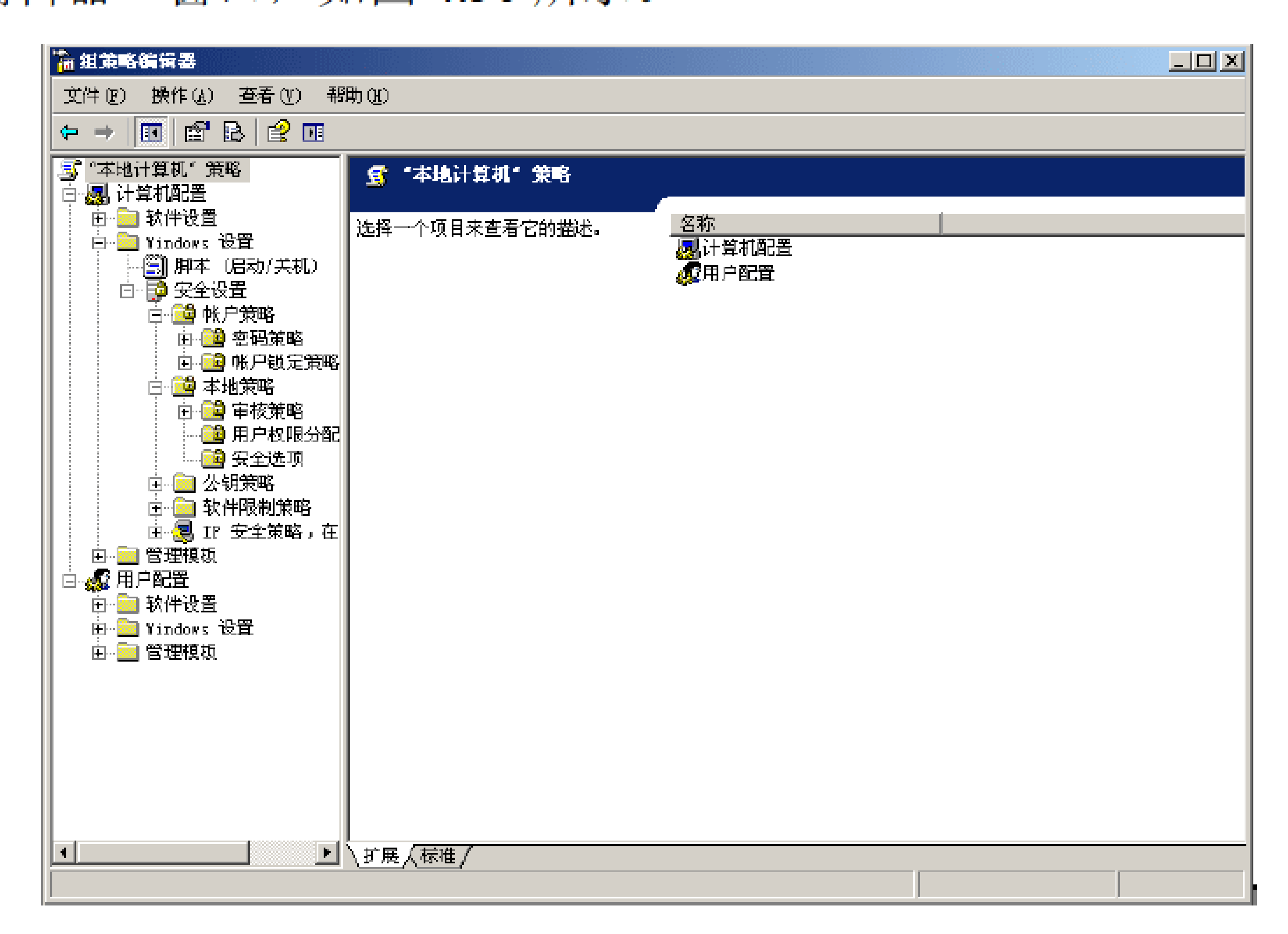


图 4.36　“组策略编辑器”窗口



第 2 步：依次展开“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”→“安全选项”文件夹，在其中完成本地策略的各种安全设置，如图 4.37 所示。双击其中的任何一个策略设置选项，将出现一个相应内容的对话框来提示操作者进行参数的输入或选择。

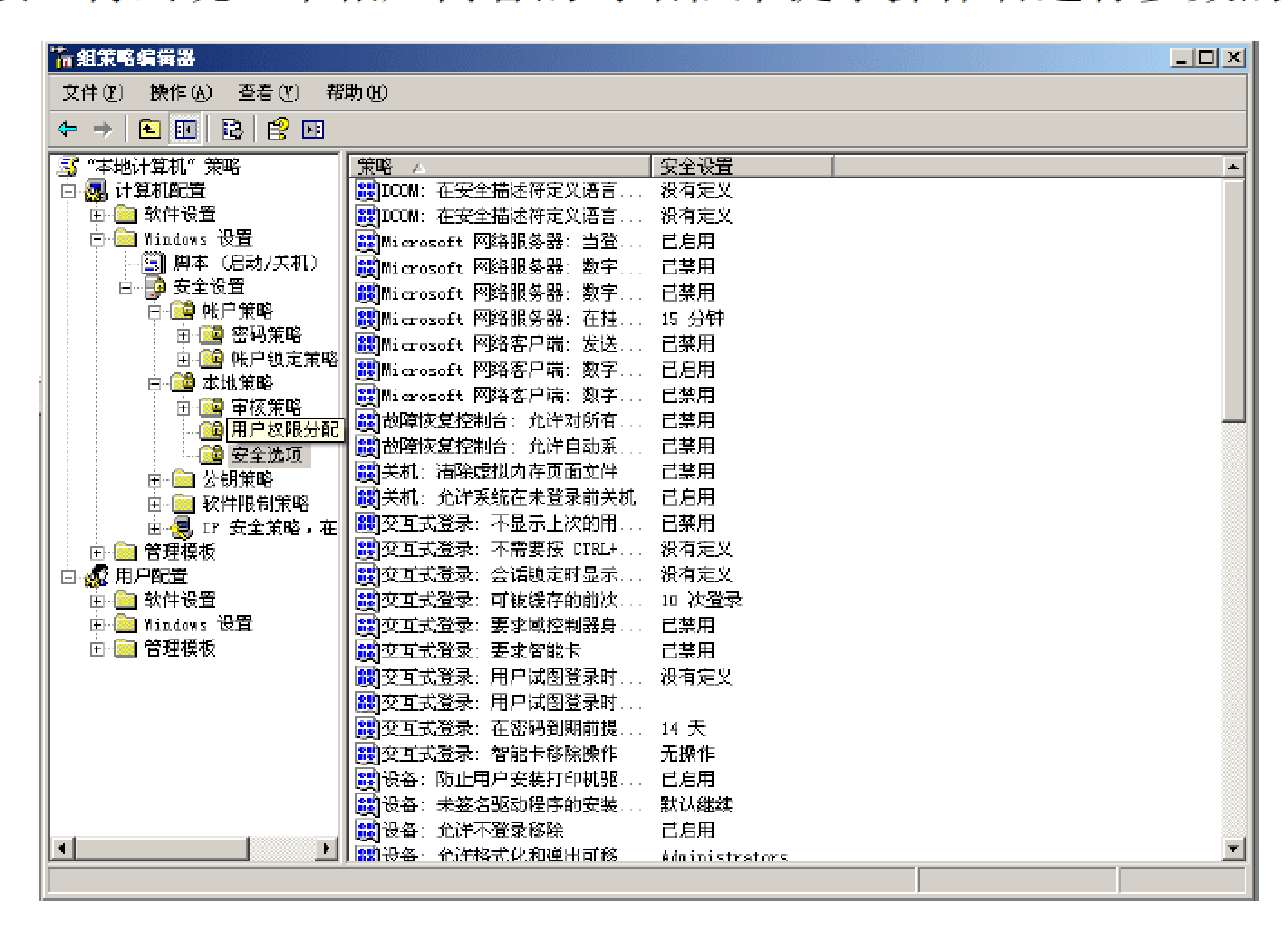


图 4.37　本地策略的各种安全设置

2.　Windows Server 2003 用户权限配置

第 1 步：执行“开始”→“运行”命令，在“打开”文本框输入 gpedit.msc 命令，单击“确定”按钮，打开“组策略编辑器”窗口。

第 2 步：在“组策略编辑器”窗口中依次展开“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”→“用户权限分配”文件夹，在其中进行本地用户权限的各种安全设置，如图 4.38 所示。

第 3 步：双击“用户权限分配”文件夹中的任何一个用户权限设置选项，将出现一个相应内容的对话框，要求操作者选择该权限的拥有者——用户或组，单击“添加用户或组”按钮即可对用户或组进行添加，而选择已有的任何一个用户或组，则可以通过单击“删除”按钮来删除该用户或组。

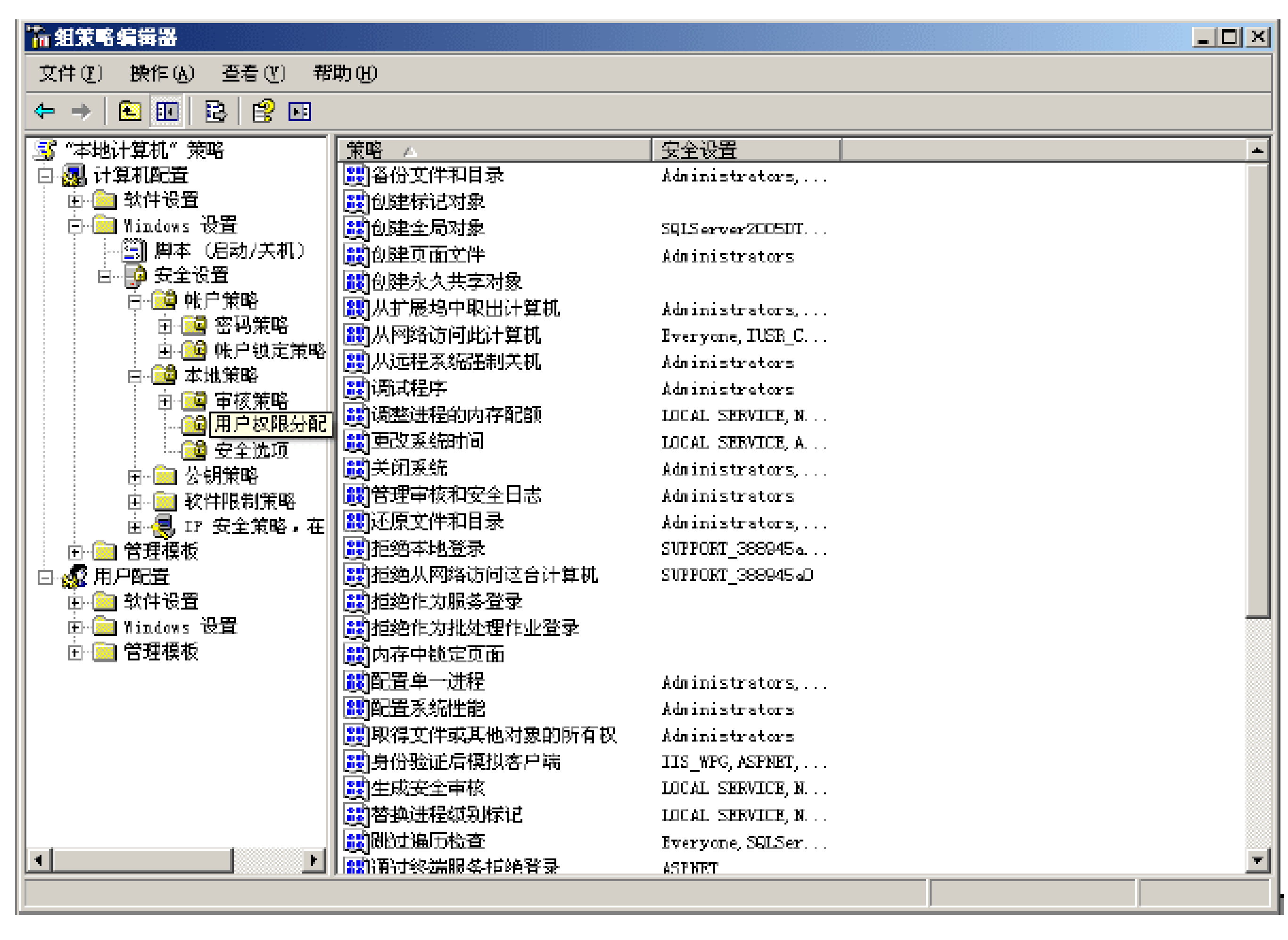


图 4.38　用户权限分配设置



第 5 章
防火墙应用技术

知识目标

- 理解防火墙的概念、功能特点及安全性。
- 掌握防火墙的分类、防火墙的系统结构。
- 了解防火墙的发展趋势。

技能目标

- 掌握常见防火墙的使用。
- 掌握常见防火墙的选购、安装和维护。

企业的内部网与 Internet 相连，方便了企业内部之间以及企业与外部的信息交流，提高了工作效率。然而，一旦企业内部网连入 Internet，就意味着 Internet 上的每个用户都有可能访问企业内部网。如果没有一个安全性保护措施，黑客们可能会在用户毫无察觉的情况下进入企业内部网，非法访问企业的资源。而防火墙就是保护企业内部网中信息安全的一项重要措施。

5.1　防火墙技术简介

防火墙（Firewall）是一种能将内部网和公众网分开的技术，它能限制被保护的网络与互联网及其他网络之间进行的信息存取、传递等操作。在构建安全的网络环境过程中，防火墙作为第一道安全防线，正受到越来越多用户的关注。

5.1.1　防火墙的概念

防火墙技术最初是针对 Internet 网络不安全因素所采取的一种保护措施。顾名思义，防火墙就是用来阻挡外部不安全因素影响内部网络的屏障，其目的就是防止外部网络用户未经授权的访问。它是一种计算机硬件和软件的结合，使 Internet 与 Intranet 之间建立起一个安全网关（Security Gateway），从而保护内部网免受非法用户的侵入。防火墙主要由服务访问政策、验证工具、包过滤和应用网关 4 个部分组成，其就是一个位于计算机和它所连接的网络之间的软件或硬件（其中硬件防火墙用的很少，只有国防部等单位才用，因为它的价格昂贵）。安装防火墙的计算机流入流出的所有网络通信均要经过此防火墙。

防火墙实际上是一种访问控制技术，它在一个被认为是安全和可信的内部网络和一个被认为是不那么安全和可信的外部网络之间设置障碍，阻止对信息资源的非法访问，也可以阻止保密信息从受保护网络上被非法输出。它能允许你“同意”的人和数据进入你的网络，同时将你“不同意”的人和数据拒之网外。换句话说，如果不通过防火墙，可信网络内部和外部的人就无法进行通信。

防火墙是一类防范措施的总称，不是一个单独的计算机程序或设备。在物理上，它通常是一组硬件设备和软件的多种组合。在逻辑上，它是分离器、限制器和分析器，可有效地监控内部网和公共网之间的任何活动。防火墙是不同网络或网络安全域之间信息的唯一出入口，能根据一定的安全政策控制出入网络的信息流。防火墙本身具有较强的抗攻击能力，是提供信息安全服务、实现网络和信息安全的基础设施。如图 5.1 所示为防火墙示意图。

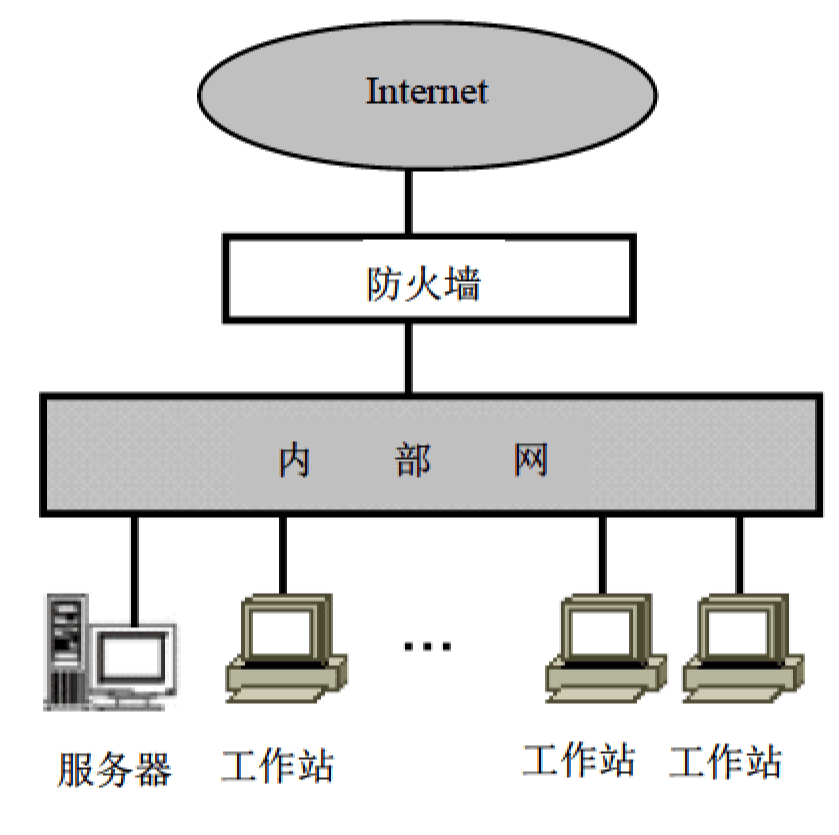


图 5.1　防火墙示意图



5.1.2 防火墙的功能

防火墙一方面对经过它的网络通信进行扫描，过滤掉一些可能攻击内部网络的数据。另一方面防火墙可以关闭不使用的端口，能禁止特定端口通信，封锁特洛伊木马。它可以禁止来自特殊站点的访问，从而防止来自不明入侵者的所有通信。具体来说，防火墙的作用主要体现在以下几个方面。

1. 防火墙是网络安全的屏障

一个防火墙（作为阻塞点、控制点）能极大地提高一个内部网络的安全性，并通过过滤不安全的服务而降低风险。由于只有经过精心选择的应用协议才能通过防火墙，所以网络环境变得更安全。如防火墙可以禁止诸如众所周知的不安全的NFS协议进出受保护网络，这样外部的攻击者就不可能利用这些脆弱的协议来攻击内部网络。防火墙同时可以保护网络免受基于路由的攻击，如IP选项中的源路由攻击和ICMP重定向中的重定向路径。防火墙应该可以拒绝所有以上类型攻击的报文并通知防火墙管理员。

2. 防火墙可以强化网络安全策略

通过以防火墙为中心的安全方案配置，能将所有安全软件（如口令、加密、身份认证、审计等）配置在防火墙上。与将网络安全问题分散到各个主机上相比，防火墙的集中安全管理更经济。例如在网络访问时，一次一密口令系统和其他的身份认证系统完全可以不必分散在各个主机上，而集中在防火墙上。

3. 网络存取和访问监控审计

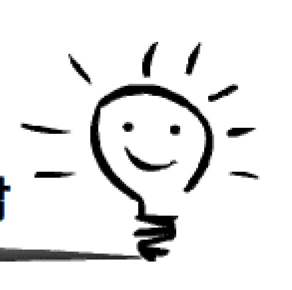
如果所有的访问都经过防火墙，那么防火墙就能记录下这些访问并作出日志记录。当发生可疑动作时，防火墙能进行适当的报警，并提供网络是否受到监测和攻击的详细信息。另外，收集一个网络的使用和误用情况也是非常重要的。首先是可以清楚防火墙是否能够抵挡攻击者的探测和攻击，并且清楚防火墙的控制是否充足。而网络使用统计对网络需求分析和威胁分析等而言也是非常重要的。

4. 防止内部信息的外泄

通过利用防火墙对内部网络的划分，可实现对内部网重点网段的隔离，从而限制了局部重点或敏感网络安全问题对全局造成的影响。再者，隐私是内部网络非常关心的问题，一个内部网络中不引人注意的细节可能包含了有关安全的线索而引起外部攻击者的兴趣，甚至因此而暴露了内部的某些安全漏洞。使用防火墙就可以隐蔽一些内部细节，如Finger、DNS等服务。Finger显示的信息非常容易被攻击者所获悉，攻击者可以知道一个系统使用的频繁程度、这个系统是否有用户正在连线上网、这个系统是否在被攻击时引起注意等。防火墙可以同样阻塞有关内部网络中的DNS信息，这样一台主机的域名和IP地址就不会被外界所了解。

5. 防火墙支持具有Internet服务特性的企业内部网络技术体系VPN

通过VPN，将企事业单位分布在全世界各地的LAN或专用子网，有机地联成一个整体，不仅省去了专用通信线路，而且为信息提供了技术保障。



5.1.3　防火墙的缺陷

尽管防火墙有许多防范功能，但由于互联网的开放性，它也有一些不尽如人意的地方。主要表现在以下几个方面：

（1）防火墙可以阻断攻击，但不能消灭攻击源。“各扫自家门前雪，不管他人瓦上霜”就是目前网络安全的现状。互联网上病毒、木马、恶意试探等造成的攻击行为络绎不绝，设置得当的防火墙能够阻挡它们，但是无法清除攻击源。即使防火墙进行了良好的设置，使得攻击无法穿透防火墙，但各种攻击依然会源源不断地向防火墙发出尝试。例如接主干网 10MB 网络带宽的某站点，其日常流量中平均有 512KB 左右的攻击行为。那么，即使成功设置了防火墙，这 512KB 的攻击流量依然不会有丝毫减少。

（2）防火墙不能抵御最新的未设置策略的攻击漏洞。就如杀毒软件与病毒一样，总是先出现病毒，杀毒软件经过分析出特征码后加入到病毒数据库内才能查杀。防火墙的各种策略，也是在该攻击方式经过专家分析后给出特征才设置的。如果新发现某个主机漏洞的黑客把第一个攻击对象选定为该主机所在的网络，那么防火墙也没有办法。

（3）防火墙的并发连接数限制容易导致拥塞或者溢出。由于要判断、处理流经防火墙的每一个包，因此防火墙在某些流量大、并发请求多的情况下，很容易导致拥塞，成为整个网络的瓶颈从而影响性能。而当防火墙溢出时，整个防线就如同虚设，原本被禁止的连接也能从容通过了。

（4）防火墙对服务器合法开放的端口的攻击大多无法阻止。某些情况下，攻击者利用服务器提供的服务进行缺陷攻击，例如利用开放了 3389 端口取得没打过 SP 补丁的 Windows 2000 的超级权限、利用 ASP 程序进行脚本攻击等。由于其行为在防火墙一级看来是“合理”和“合法”的，由此就被简单地放行了。

5.1.4　防火墙技术的发展趋势

随着新的网络工具的出现，防火墙技术也有一些新的发展趋势。这主要可以从包过滤技术、防火墙体系结构和防火墙系统管理 3 方面来体现。

1. 防火墙包过滤技术发展趋势

（1）一些防火墙厂商把在 AAA 系统上运用的用户认证及其服务器扩展到防火墙中，使其拥有可以支持基于用户角色的安全策略功能。该功能在无线网络应用中非常必要。具有用户身份验证的防火墙通常是采用应用级网管技术的，包过滤技术的防火墙不具有。用户身份验证功能越强，它的安全级别越高，但它给网络通信带来的负面影响也越大，因为用户身份验证需要时间，特别是加密型的用户身份验证。

（2）多级过滤技术。是指防火墙采用多级过滤措施，并辅以鉴别手段。在分组过滤（网络层）一级，过滤掉所有的源路由分组和假冒的 IP 源地址；在传输层一级，遵循过滤规则，过滤掉所有禁止出或入的协议和有害数据包，如 nuke 包、圣诞树包等；在应用网关（应用层）一级，能够利用 FTP、SMTP 等各种网关，控制和监测 Internet 提供的所用通用服务。这是针对以上各种已有防火墙技术的不足而产生的一种综合型过滤技术，它可以弥补以上



各种单独过滤技术的不足。

（3）使防火墙具有病毒防护功能。现在通常被称之为病毒防火墙，当然目前主要还是在个人防火墙中体现，因为它是纯软件形式，更容易实现。这种防火墙技术可以有效地防止病毒在网络中的传播，比等待攻击的发生更加积极。拥有病毒防护功能的防火墙可以大大减少公司的损失。

2. 防火墙的体系结构发展趋势

随着网络应用的增加，对网络宽带提出了更高的要求，这意味着防火墙要能够以非常高的速率处理数据。另外，在以后几年里，多媒体应用将会越来越普通，它要求数据穿过防火墙所带来的延迟要足够小。为了满足这种需要，一些防火墙制造商开发了基于 ASCI 的防火墙和基于网络处理器的防火墙。从执行速度的角度来看，基于网络处理器的防火墙也是基于软件的解决方案，它需要在很大程度上依赖于软件的性能，但是由于这类防火墙中有一些专门用于处理数据层面任务的引擎，从而减轻了 CPU 的负担，该类防火墙的性能要比传统防火墙的性能好许多。

与基于 ASIC 的纯硬件防火墙相比，基于网络处理器的防火墙具有软件色彩，因而更加具有灵活性。

基于 ASIC 的防火墙使用专门的硬件处理网络数据流，比起前两种的防火墙具有更好的性能，但是纯硬件的 ASIC 防火墙缺乏可编程性，这就使得它缺乏灵活性，从而跟不上防火墙功能的快速发展。理想的解决方案是增加 ASIC 芯片的可编程性，使其与软件更好地配合。这样的防火墙就可以同时满足来自灵活性和运行性能的要求。

3. 防火墙的系统管理发展趋势

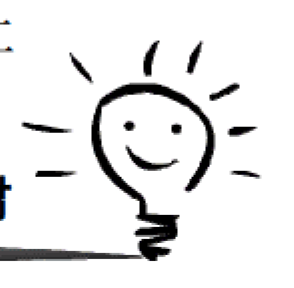
（1）首先是集中式管理，分布式和分层的安全结构是将来的趋势。集中式管理可以降低管理成本，并保证在大型网络安全策略上的一致性。快速响应和快速防御也要求采用集中式管理系统。目前这种分布式防火墙早已在 Cisco、3Com 等大的网络设备开发商中开放成果，也就是目前所称的分布式防火墙和嵌入式防火墙。

（2）强大的审计功能和自动日志分析功能。这两点的应用可以更早地发现潜在的威胁并预防攻击的发生。日志功能还可以让管理员有效地发现系统中存在的安全漏洞，及时地调整安全策略等各方面管理，具有非常大的帮助。不过具有这种功能的防火墙通常是比较高级的，早期的静态包过滤防火墙不具有这种功能。

（3）随着网络安全技术的发展，现在有一种说法，叫做建立以防火墙为核心的网络安全体系。因为在现实中发现，仅现有的防火墙技术难以满足当前网络安全需求，通过建立一个以防火墙为核心的安全体系，就可以为内部网络系统部署多道安全防线，各种安全技术各司其职，从各方面防御外来入侵。

5.2 防火墙技术的分类

防火墙是近期发展起来的一种保护计算机网络安全的技术性措施，它是一个用以阻止



网络中的黑客访问某个机构网络的屏障，在网络边界上通过建立起来的相应网络监控系统来隔离内部和外部网络，以阻挡外部网络的侵入。目前的防火墙主要有两大类，即包过滤防火墙和代理防火墙。

5.2.1　包过滤防火墙技术

1. 包过滤防火墙技术

包过滤（Packet Filtering）技术是防火墙为系统提供安全保障的主要技术，它依据系统内事先设定的过滤逻辑，通过设备对进出网络的数据流进行有选择的控制与操作。

包过滤技术作为防火墙的应用有 3 种：第一种是路由设备在完成路由选择和数据转发的同时进行包过滤；第二种是在工作站上使用软件进行包过滤；第三种是在一种称为屏蔽路由器的路由设备上启动包过滤功能。目前较常用的方式是第一种。用户可以设定一系列的规则，指定允许哪些类型的数据包可以流入或流出内部网络，哪些类型的数据包的传输应该被拦截。

包过滤技术作用在网络层和传输层，以 IP 包信息为基础，对通过防火墙的 IP 包的源、目的地址、TCP/UDP 的端口标识符及 ICMP 等进行检查。规定了哪些网络节点何时可通过防火墙访问外部网络；哪些网络节点可访问内部网络，或者哪些用户只能使用 E-mail，而不能使用 Telnet 和 FTP；哪些用户只能使用 Telnet，而不能使用 FTP 等。可以利用安全策略形式语言描述安全配置规则，并进行一致性检查，达到方便配置安全策略的目的。

包过滤规则检查数据流中每个数据包后，根据规则来确定是否允许数据包通过，其核心是过滤算法的设计。如果包的出入接口相匹配，并且规则允许该数据包通过，那么该数据包就会按照路由表中的信息被转发。但是，如果包的出入接口相匹配，而规则拒绝该数据包，那么该数据包也会被丢弃。如果出入接口未设匹配规则，用户配置的默认参数会决定是转发还是丢弃数据包。

数据包过滤在网络中起着举足轻重的作用，它允许用户在某个地方为整个网络提供特别的保护。例如，Telnet 服务器在 TCP 的 23 号端口上监听远程连接，而 SMTP 服务器在 TCP 的 25 号端口上监听连接。为了阻塞所有进入的 Telnet 连接，包过滤路由器只需要简单地丢弃所有 TCP 端口号等于 23 的数据包。为了将进来的 Telnet 连接限制在内部的数台机器上，包过滤路由器必须拒绝所有 TCP 端口号等于 23，并且目标 IP 地址不等于允许主机的 IP 地址的数据包。

包过滤操作可以在路由器上进行，也可以在网桥，甚至在一个单独的主机上进行，大多数数据包过滤系统不处理数据本身，它们不根据数据包的内容做决定。

2. 包过滤防火墙技术的优缺点

包过滤防火墙技术有很多优点，主要体现在以下几点。

（1）包过滤技术不用改动客户机和主机上的应用程序，因为过滤发生在网络层和传输层，与应用无关。

（2）单独的、恰当的放置数据包过滤路由器有助于整个网络。如果仅有一个路由器连



接内部网络和外部网络，那么不论网络大小、拓扑结构如何，所有网络通信都要通过那个路由器进行数据包过滤，这样在网络安全方面就能取得较好的效果。

（3）数据包过滤技术对用户没有特别的要求。它是在 IP 层实现的，不要求任何自定义的软件或者特别客户机配置，也不要求用户经过任何特殊训练。当数据包过滤路由器在检查数据包时，它与普通路由器没什么区别，甚至用户感觉不到它的存在，除非用户试图做一些数据包过滤路由器所禁止的事。这样，数据包过滤技术对用户来说，具有较强的透明度，使用起来很方便。

（4）大多数路由器都具有数据包过滤功能，无论是商业的还是免费的，许多硬件或软件路由产品都具有数据包过滤能力，大多数网络使用的路由器也具有这种功能。数据包过滤路由器工作时一般只检查报头相应的字段，而不查看数据包的内容，而且有些核心部件是由专用硬件实现的，所以转发速度快，效率比较高。

由以上优点可以看出，数据包过滤是一种通用、廉价、有效的安全手段，说它通用是因为它不针对各个具体的网络服务采取特殊的处理方式；说它廉价是因为大多数路由器都提供分组过滤功能；说它有效是因为它在很大程度上满足了企业的安全要求。

数据包过滤技术存在的缺陷主要体现在以下几点。

（1）在过滤过程中判别的只有网络层和传输层的有限信息，而不能在用户级别上进行过滤，不能识别不同的用户和防止 IP 地址的盗用，因而各种安全要求不可能充分满足。例如，攻击者可以把自己主机的 IP 地址设成一个合法主机的 IP 地址，这样就可以很轻易地通过报文过滤器。

（2）在许多过滤器中，过滤规则的数目是有限制的，随着规则数目的增加，设备性能会受到很大地影响，导致用户难以使用某些需要的规则。例如，它们只能确定数据包来自什么主机，而不能指定到达特定的应用程序，当用户通过端口号对一些协议实行限制时，其他的协议同时也被禁止了。

（3）当前的过滤工具并不完善，或多或少的存在一些局限性。如数据包过滤规则难以配置，甚至不可能运行；难以检查数据包过滤规则；许多产品的数据包过滤能力不足等。

（4）由于缺少上下文关联信息，数据包过滤路由器不能有效地过滤诸如 UDP、RPC、FTP 一类的协议。

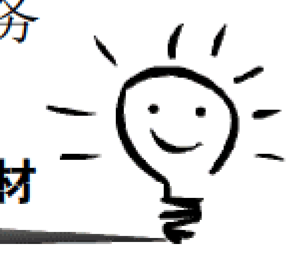
（5）数据包过滤技术对安全管理人员素质要求较高。建立安全规则时，管理人员必须对协议本身及其在不同应用程序中的作用有较深入的理解。

在实际应用中，很少把数据包过滤技术当作单独的安全解决方案，主要是因为数据包过滤技术本身的缺陷。包过滤路由器通常是和应用网关配合或是与其他防火墙技术一起使用，共同组成防火墙系统。

5.2.2 代理防火墙技术

1. 代理防火墙技术

代理防火墙技术主要是代理服务器（Proxy Server）。代理服务器是指代理内部网络用户与外部网络服务器进行信息交换的程序。它可以将内部用户的请求确认后送达外部服务



器，同时将外部服务器的响应再送给用户。这种技术经常被用于在 Web 服务器上高速缓存信息，扮演着 Web 客户和 Web 服务器之间的中介角色。它主要保存 Internet 上最常用和最近访问过的内容，可为用户提供更快的访问速度，并且提高了网络安全性。由于代理服务器在外部网络向内部网络申请服务时发挥了中间转接和隔离的作用，因此又把它叫做代理防火墙。

代理防火墙作用在应用层，用来提供应用层服务的控制，其特点是完全阻隔了网络通信流。通过对每种应用服务编制专门的代理程序，实现监视和控制应用层通信流的作用，所以代理防火墙又被称为应用代理或应用层网关型防火墙。

应用层网关型防火墙控制的内部网络只接受代理服务器提出的服务请求，拒绝外部网络其他节点的直接请求。它同时提供了多种方法认证用户。当确认了用户名和口令后，服务器根据系统的设置对用户作进一步的检查，验证其是否可以访问本服务器。应用层网关型防火墙还对进出防火墙的信息进行记录，并可由网络管理员用来监视和管理防火墙的使用情况，实际中的应用网关通常由专用代理服务器实现。如图 5.2 所示为代理防火墙的示意图。

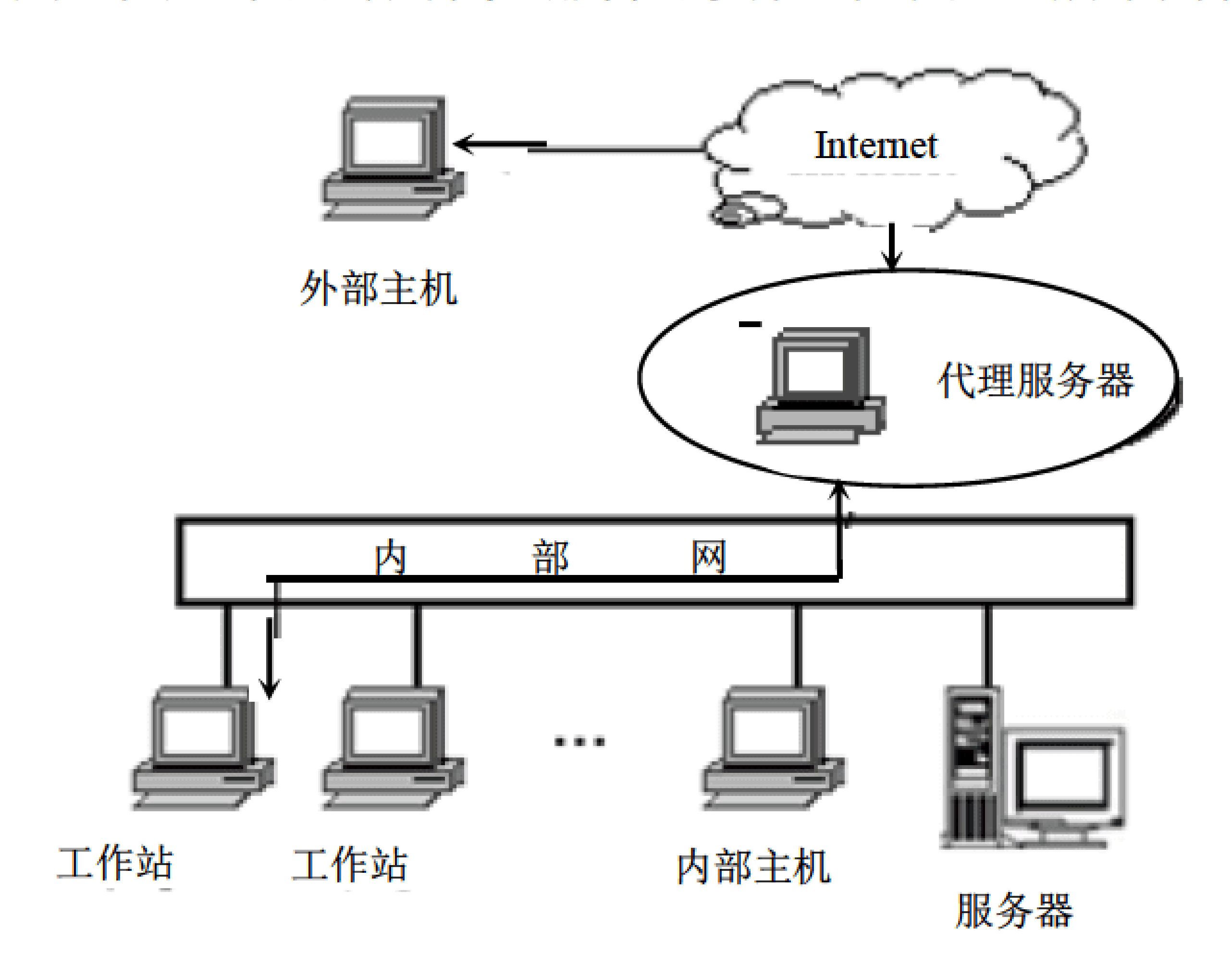


图 5.2　代理防火墙的示意图

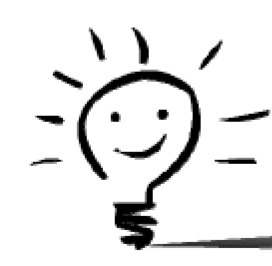
具体来说，应用层网关是内部网与外部网的隔离点，掌握着应用系统中可用做安全决策的全部信息，这使得网络管理员能够实现比包过滤路由器更严格的安全策略。应用层网关不用依赖包过滤工具来管理 Internet 服务在防火墙系统中的进出，而是采用为每种所需服务安装特殊代码的方式来管理 Internet 服务。如果网络管理员没有为某种应用安装代理编码，那么该项服务就不被支持并不能通过防火墙系统来转发。同时，代码还可以配置成只支持网络管理员认为必须的部分功能，从而有效地防止网络攻击。

2. 代理防火墙技术的优缺点

代理防火墙技术的优点如下。

（1）代理能生成各项记录。因为代理工作在应用层，它检查各项数据，可以按一定准则，让代理生成各项日志、记录。这些日志、记录对于流量分析、安全检验是十分重要和宝贵的。当然，它也可以用于计费等。

（2）代理易于配置。代理因为是一个软件，所以它较路由器更易配置。配置界面十分



友好。如果代理实现得好，可以对配置协议要求较低，从而避免了配置错误。

（3）代理能灵活、完全地控制进出流量、内容。通过采取一定措施，按照一定的规则，用户可以借助代理实现一整套的安全策略，比如可控制谁和什么时间、地点。

（4）代理能过滤数据内容。用户可以把一些过滤规则应用于代理，让它在高层实现过滤功能，例如文本过滤、图像过滤（目前还未实现，但这是一个热点研究领域）、预防病毒或扫描病毒等。

（5）代理可以方便地与其他安全手段集成。目前的安全问题解决方案很多，如认证、授权、账户、数据加密、安全协议等。如果把代理与这些手段联合使用，将大大增加网络安全性。

代理防火墙技术的缺点如下。

（1）代理对用户不透明，大多代理要求客户端做相应改动或安装定制客户端软件，这给用户增加了不透明度。为庞大的互联网络中的每一台内部主机安装和配置特定的应用程序既消耗时间，又容易出错，因为它们的硬件平台和操作系统都存在差异。

（2）代理速度比路由器慢。路由器只是简单地查看 TCP/IP 报头，检查特定的几个域，不做详细分析、记录，而代理工作于应用层，要检查数据包的内容，按特定的应用协议进行审查、扫描数据包内容，并进行转发请求或响应，所以速度较慢。

（3）对于每项服务代理可能要求不同的服务器，可能需要为每项协议设置一个不同的代理服务器。因为代理服务器不得不理解协议以便判断什么是允许的和不允许的，并且还装扮成一个对真实服务器来说是客户，对代理客户来说是服务器的角色，挑选、安装和配置这些不同服务器也可能是一项较复杂的工作。

（4）除了一些为代理而设的服务处，代理服务器要求对客户或过程进行限制，每一种限制都有不足之处，人们无法经常按他们自己的步骤使用快捷可用的工具。由于这些限制，代理应用就不能像非代理应用运行的那么好，它们往往可能曲解协议的说明，并且一些客户和服务器比其他的要缺少一些灵活性。

（5）代理服务器不能保证免受所有协议弱点的限制。作为一个安全问题的解决方法，代理取决于对协议中哪些是安全操作的判断能力。每个应用层协议，都或多或少地存在一些安全问题，对于一个代理服务器来说，要彻底避免这些安全隐患几乎是不可能的，除非关掉这些服务。代理取决于在客户端和真实服务器之间插入代理服务器的能力，这要求两者之间交流的相对直接性，而且有些服务的代理是相当复杂的。

（6）代理不能改进底层协议的安全性。因为代理工作于应用层，所以它不能提高底层通信协议的能力。而这些方面，对于一个网络的健壮性是相当重要的。

在实际应用中，构筑防火墙的解决方案很少采用单一的技术，大多数防火墙是将包过滤技术和代理服务器结合起来使用的。

5.3 常见的防火墙系统结构

出于对更高安全性的要求，通常的防火墙系统是多种解决不同问题的技术的有机组合。



例如，把基于包过滤的方法与基于应用代理的方法结合起来，就形成了复合型防火墙产品。目前常见的有以下几种配置方法。

1. 屏蔽路由器

屏蔽路由器是防火墙最基本的构件，是最简单也是最常见的防火墙。屏蔽路由器作为内外连接的唯一通道，要求所有的报文都必须在此通过检查。路由器上可以安装基于 IP 层的报文过滤软件，实现报文过滤功能。许多路由器本身带有报文过滤配置选项，但一般比较简单。

这种配置的优点是容易实现、费用少，并且对用户的要求较少，使用方便。其缺点是日志记录能力不强，规则表庞大、复杂，整个系统依靠单一的部件来进行保护，一旦被攻击，系统管理员很难确定系统是否正在被入侵或已经被入侵了。

2. 双宿主主机网关

双宿主主机是一台安装有两块网卡的计算机，每块网卡有各自的 IP 地址，并分别与受保护网和外部网相连。如果外部网络上的计算机想与内部网络上的计算机进行通信，它就必须与双宿主主机上与外部相连的 IP 地址联系，代理服务器软件再通过另一块网卡与内部网络相连接。也就是说，外部网络与内部网络不能直接通信，它们之间的通信必须经过双宿主主机的过滤和控制，如图 5.3 所示。

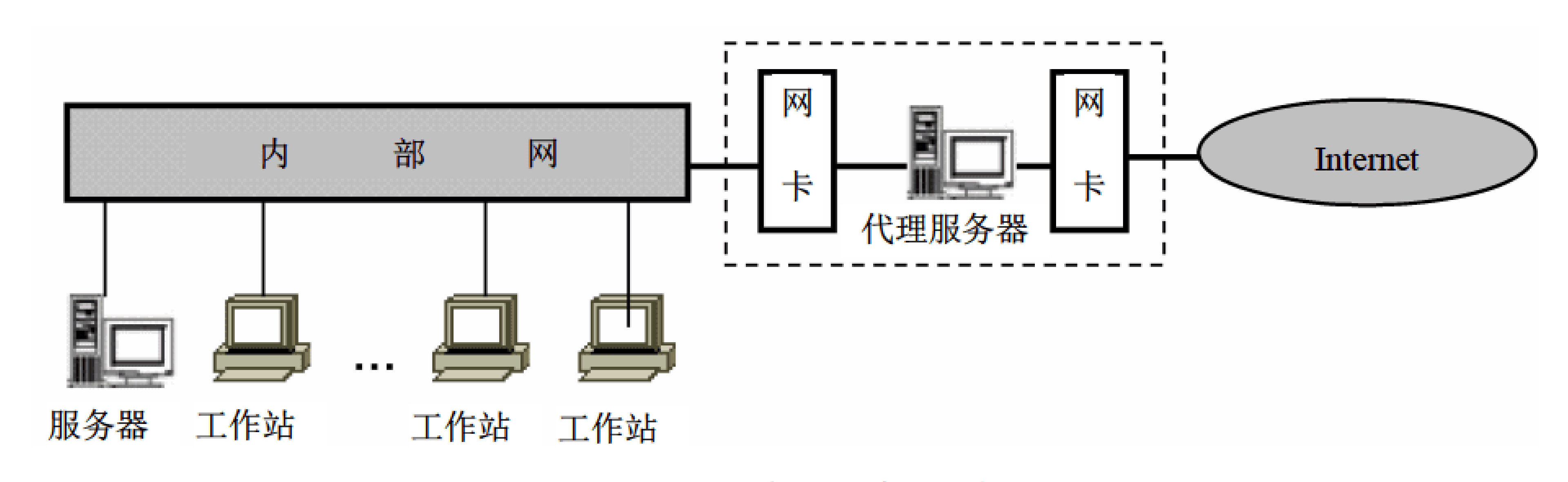


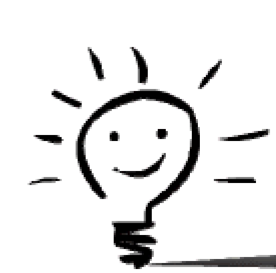
图 5.3　双宿主主机网关

这种配置是用双宿主主机做防火墙，两块网卡各自在主机上运行着防火墙软件，可以转发应用程序、提供服务等。应该指出的是，在建立双宿主主机时，应该关闭操作系统的路由能力，否则从一块网卡到另一块网卡的通信会绕过代理服务器软件，而使双宿主主机网关失去“防火”的作用。

这种配置的优点是网关可将受保护网络与外界完全隔离；代理服务器可提供日志，有助于网络管理员确认哪些主机可能已被入侵；同时，由于它本身是一台主机，所以可用于诸如身份验证服务器及代理服务器，使其具有多种功能。它的缺点是双宿主主机的每项服务必须使用专门设计的代理服务器，即使较新的代理服务器能处理几种服务，也不能同时进行；另外，一旦双宿主主机受到攻击，并使其只具有路由功能，那么任何网上用户都可以随便访问内部网络了，这将严重损害网络的安全性。

3. 屏蔽主机网关

屏蔽主机网关由屏蔽路由器和应用网关组成，屏蔽路由器的作用是包过滤，应用网关



的作用是代理服务。这样，在内部网络和外部网络之间建立了两道安全屏障，既实现了网络层安全，又实现了应用层安全。来自外部网络的所有通信都会连接到屏蔽路由器，它根据所设置的规则过滤这些通信。在多数情况下，与应用网关之外的机器的通信都会被拒绝。网关的代理服务器软件用自己的规则，将被允许的通信传送到受保护的网络上。在这种情况下，应用网关只有一块网卡，因此它不是双宿主主机网关，如图 5.4 所示。

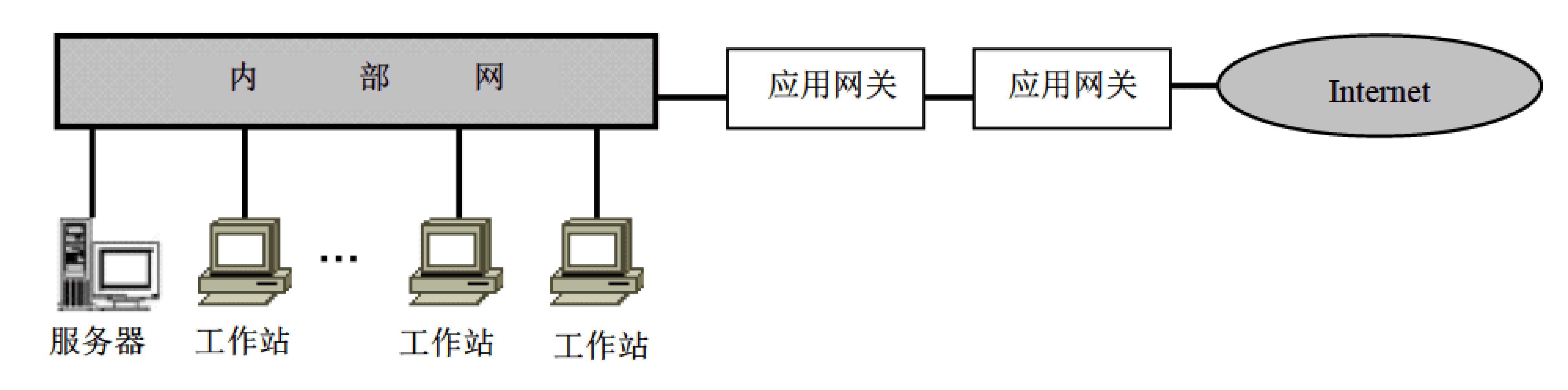


图 5.4　屏蔽主机网关

屏蔽主机网关比双宿主主机网关设置更加灵活，它可以设置成使屏蔽路由器将某些通信直接传到内部网络的站点，而不是传到应用层网关。另外，屏蔽主机网关具有双重保护，安全性更高。它的缺点主要是由于要求对两个部件配置，使它们能协同工作，所以屏蔽主机的主机将失去任何的安全保护，使整个网络对攻击者敞开。

4. *屏蔽子网*

屏蔽子网系统结构是在屏蔽主机网关的基础上再加上一个屏蔽路由器，两个路由器放在子网的两端，三者形成了一个被称为“非军事区”的子网，如图 5.5 所示。

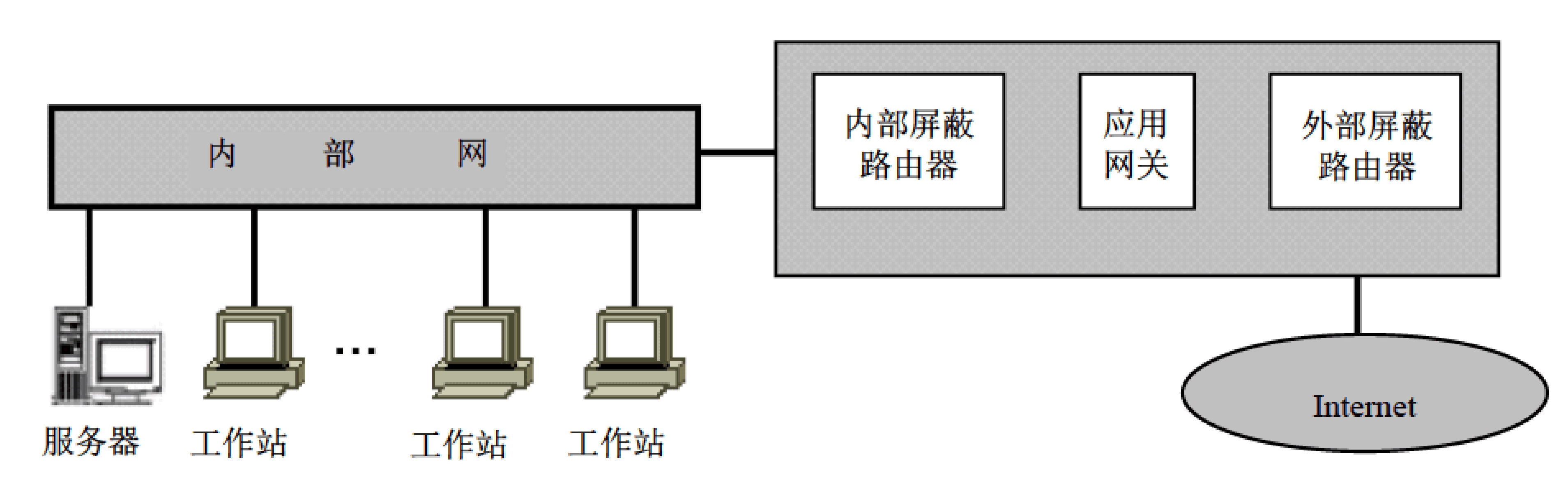


图 5.5　屏蔽子网

这种方法在内部网络和外部网络之间建立了一个被隔离的子网。用两台屏蔽路由器将这一子网分别与内部网络和外部网络分开。内部网络和外部网络均可访问屏蔽子网，但禁止它们穿过屏蔽子网通信。外部屏蔽路由器和应用网关与在屏蔽主机网关中的功能相同，内部屏蔽路由器在应用网关和受保护网络之间提供附加保护。为了入侵用这种体系结构构筑的内部网络，攻击者必须通过两个路由器。即使攻击者成功入侵了应用网关，他仍将面对内部路由器，这就消除了内部网络的单一入侵点。在屏蔽子网防火墙系统结构中，应用网关和屏蔽路由器共同构成了整个防火墙的安全基础。

屏蔽子网防火墙系统结构的不足是，它要求的设备和软件模块是上述几种防火墙系统结构中最多的，其配置也相当复杂和昂贵。



5.4　防火墙选购策略

选用防火墙首先要明确哪些数据是必须保护的，这些数据被入侵会导致什么样的后果及网络不同区域需要什么等级的安全级别。因此，首先要根据信息系统安全级别确定；其次才是防火墙的功能，选用防火墙必须与网络接口匹配，要阻止你所能想到的威胁，防火墙可以是软件或硬件模块，并能集成于网桥、网关、路由器等设备之中。防火墙的选购原则主要有以下几方面。

1．防火墙自身的安全性

大多数人在选择防火墙时都将注意力放在防火墙如何控制连接以及防火墙支持多少种服务上，但往往忽略一点，防火墙也是网络上的主机设备，也可能存在安全问题。防火墙如果不能确保自身安全，则防火墙的控制功能再强也终究不能安全保护内部网络。

通常防火墙都安装在一般的操作系统（如 UNIX、Windows Server 2003 等）上。在防火墙主机上执行的除了防火墙软件外，所有的程序、系统核心，也大多来自操作系统本身的原有程序。当防火墙上所执行的软件出现安全漏洞时，防火墙本身也将受到威胁。此时，任何的防火墙控制机制都可能失效，因为当一个黑客取得了防火墙上的控制权以后，黑客几乎可以为所欲为地修改防火墙上的存取规则，进而入侵更多的系统。因此，防火墙自身应有相当高的安全保护。

2．应考虑的特殊需求

企业安全策略中往往有些特殊需求，不是每一个防火墙都会提供的，这是选择防火墙需考虑的因素之一。常见的需求如下：

（1）IP 转换。

进行 IP 转换有两个好处：其一是隐藏内部网络真正的 IP，这可以使黑客无法直接攻击内部网络，也是要强调防火墙自身安全性问题的主要原因；另一个好处是可以让内部网络保留 IP，这对许多 IP 不足的企业是有益的。

（2）双重 DNS。

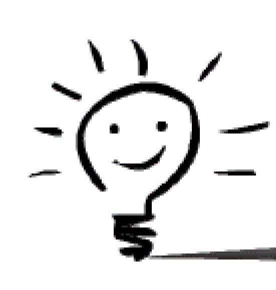
当内部网络使用没有注册的 IP 地址或是防火墙进行 IP 转换时，DNS 也必须经过转换。因为，同样的一个主机在内部的 IP 与给予外界的 IP 将会不同，有的防火墙会提供双重 DNS，有的则必须在不同主机上各安装一个 DNS。

（3）虚拟专用网络（VPN）。

VPN 可以在防火墙与防火墙或移动的 Client 间对所有网络传输的内容加密，建立一个虚拟通道，让两者间感觉是在同一个网络上，可以安全且不受拘束地互相存取，这对总公司与分公司之间或公司与外出的员工之间，需要直接联系又不愿花费大量金钱申请专线或用长途电话拨号连接时，将会非常有用。

（4）扫毒功能。

大部分防火墙都可以与防病毒防火墙搭配实现扫毒功能。有的防火墙则可以直接集成



扫毒功能，差别只是扫毒工作是由防火墙完成，或是由另一台专用的计算机完成。

（5）特殊控制需求。

有时候企业会有特别的控制需求，如限制特定使用者才能发送 E-mail，FTP 只能 GET 档案不能 PUT 档案，限制同时上网人数，还有使用时间或 Block Java、ActiveX 等，依需求不同而定。

3. 防火墙系统的稳定性和可靠性

就一个成熟的产品来说，保障系统的稳定性是最基本的要求。目前，由于种种原因，国内有些防火墙尚未最后定型或没有经过严格的、大量的测试就被推向了市场，这样一来，其稳定性就可想而知了。防火墙的稳定性情况从厂家的宣传材料中是看不出来的，但可以从以下的一些渠道获得，如国家权威的测评认证机构、对产品的咨询、调查及试用、厂商开发研制的历史及实力等方面。

可靠性对防火墙设备来说尤为重要，其直接影响受控制网络的可用性。提高可靠性的措施一般是提高本身部件的强健性、增大设计阈值和增加冗余部件，这要求有较高的生产标准和设计冗余度，如使用工业标准、电源热备份、系统热备份等。

4. 防火墙的性能

高性能是防火墙的一个重要指标，它直接体现了防火墙的可用性，也体现了用户使用防火墙所需付出的安全代价。如果由于使用防火墙而带来了网络性能较大幅度下降，就意味着安全代价过高，用户是无法接受的。一般来说，防火墙加载上百条规则后，其性能下降不应超过 5%。

对通信行为的有效控制，要求防火墙设备有一系列不同级别，以满足不同用户的各类安全控制需求。防火墙控制的有效性、多样性、级别目标的清晰性、制定的难易性和经济性等，体现着防火墙的高效和质量。例如对普通用户，只要对 IP 地址进行过滤即可；如果是内部有不同安全级别的子网，有时则必须允许高级别子网对低级别子网进行单向访问；如果还有移动用户的话，还要求能根据用户身份进行过滤。

防火墙过滤报文时，最基础的是针对 IP 地址进行过滤。而 IP 地址是非常容易修改的，只要打听到内部网里谁可以穿过防火墙，那么将自己的 IP 地址改成与他的一样就可以了。这就需要一个针对用户身份而不是 IP 地址进行过滤的办法。目前防火墙上常用的一次性口令验证机制，通过特殊的算法，保证用户在登录防火墙时，口令不会在网络上泄露，这样，防火墙就可以确认登录上来的用户确实与他所声称的一致。

用户的网络不是一成不变的，防火墙现在可能主要是在内部网和外部网之间进行过滤，随着网络的发展，内部网络可能出现具有不同安全级别的子网，这时就需要在子网之间过滤。因此，在购买防火墙时必须清楚是否可以增加网络接口、是否具有扩展性。

随着网络技术的发展和黑客攻击手段的不断变化，防火墙也必须不断地进行升级，此时支持软件升级就很重要了。如果不支持软件升级的话，为了抵御新的攻击手段，用户就必须进行硬件上的更换，而在更换期间你的网络是不设防的，同时你也要为此花费更多的钱。



5．防火墙配置的方便性

在网络入口和出口处安装新的网络设备是比较复杂的，这意味着必须修改几乎所有现有设备的配置，因此，应选用方便配置的、支持透明通信的防火墙。它在安装时不需要对原网络配置做任何改动，所做的工作只相当于连接一个网桥或 HUB。需要时，两端连线就可以工作；不需要时，将网线恢复原状即可。

防火墙的管理在充分考虑安全需要的前提下，必须提供更方便灵活的管理方式和方法，通常体现为管理途径、管理工具和管理权限。防火墙设备首先是一个网络通信设备，管理途径的提供要兼顾通常网络设备的管理方式。管理工具主要为 GUI 类管理器，用它管理很直观，这对于设备的初期管理和不太熟悉的管理人员来说是一种有效的管理方式。权限管理是管理本身的基础，但是，应防止严格的权限认证可能带来的管理方便性的降低。

以上就是选购防火墙时需要注意的一些问题，同时要明白，没有一种技术可以百分之百地解决网络上的所有问题。网络安全会受到许多因素的影响，诸如安全策略、职员的技术背景、费用以及估计可能受到的攻击等。只有正确地认识防火墙，合理使用，才是最安全的。

5.5　防火墙实例

5.5.1　常见的防火墙软件介绍

防火墙是网络安全中重要的第一防线，越来越多的人认识到安装防火墙的重要性。下面介绍几个防火墙软件产品，这些产品的生产厂家都获得了国际计算机安全协会的认证资格，所以不需要测试网络抵御攻击的能力。

1．Check Point Firewall-1

Check Point（http://www.checkpoint.com）公司推出的 Firewall-1 共支持两个平台：一个是 UNIX 平台；另一个是 Windows NT 平台。Firewall-1 具有一种很特别的结构，称为多层次状态监视结构。这种结构让 Firewall-1 可以对复杂的网络应用软件进行快速支持。也因为这个功能，使得 Check Point 也提供了一套 APL 供开发者使用，以便开发更多的辅助工具。

Firewall-1 提供了最佳权限控制、最佳综合性能及简单明了的管理。除了 NAT 外，它还具有用户认证功能。对于 FTP，可以根据 put、set 以及文件名加以限制。对于 SMTP，它可以丢弃超过一定大小的邮件、对邮件进行病毒扫描，以及改写邮件头信息。Firewall-1 还可以防止有害 SMTP 命令（如 Debug）的执行。

Firewall-1 的用户界面是网络控制中心，定义和实施复杂的安全规则非常容易。每个规则还有一个域用于文档记录，如为什么制定这条规则，何时制定及由谁制定。

2．赛门铁克（Symantec）防火墙 SGS5660

赛门铁克（Symantec）防火墙 SGS5660 是赛门铁克（Symantec）公司系列防火墙产品



之一。属于大中小企业级千兆防火墙，具有 10 个自适应（10/100/1000M）以太网端口，最大吞吐量为 3Gbps，支持 VPN、入侵检测、日志管理、网关防病毒、入侵防御、内容过滤、防垃圾邮件。

在功能特点上，赛门铁克（Symantec）防火墙 SGS5660 支持 AES and 3DES 加密技术，支持×DSL、有线调制解调器、POP3 代理、VLAN、802.1Q VLAN trunk、动态路由协议以及简化的 GUI，管理更加方便，增强了 IPS 功能和签名机制，增强了垃圾邮件和内容过滤功能。

5.5.2 天网防火墙个人版简介

天网防火墙是我国首个达到国际一流水平，首批获得国家信息安全认证中心、国家公安部、国家安全部认证的软硬件一体化网络安全产品，性能指标及技术指标达到世界同类产品先进水平。天网防火墙发展到现在，已经在多项网络安全关键技术上取得重大突破，特别是强大的 DOS 防御功能足以傲视同行。

天网防火墙个人版是个人电脑使用的网络安全程序，根据管理者设定的安全规则把守网络，提供强大的访问控制、信息过滤等功能，帮助用户抵挡网络入侵和攻击，防止信息泄露。天网防火墙把网络分为本地网和互联网，可针对来自不同网络的信息，来设置不同的安全方案，适合于任何方式上网的用户。

（1）严密的实时监控。

天网防火墙个人版对所有来自外部机器的访问请求进行过滤，发现非授权的访问请求后立即拒绝，随时保护用户系统的信息安全。

（2）灵活的安全规则。

天网防火墙个人版设置了一系列安全规则，允许特定主机的相应服务，拒绝其他主机的访问要求。用户还可以根据自己的实际情况，添加、删除、修改安全规则，保护本机安全。

（3）应用程序规则设置。

新版的天网防火墙增加对应用程序数据包进行底层分析拦截的功能，它可以控制应用程序发送和接收数据包的类型、通信端口，并且决定拦截还是通过，这是目前其他很多软件防火墙不具有的功能。

（4）详细的访问记录和完善的报警系统。

天网防火墙个人版可显示所有被拦截的访问记录，包括访问的时间、来源、类型、代码等，用户可以清楚地看到是否有入侵者想连接到自己的机器，从而制定更有效的防护规则。与以往的版本相比，天网防火墙个人版设置了完善的声音报警系统，当出现异常情况时，系统会发出预警信号，从而让用户做好防御措施。

本章小结

防火墙是用于保护计算机网络中敏感数据不被窃取和篡改的计算机软硬件系统。

防火墙技术分为包过滤防火墙技术和代理防火墙技术。

防火墙体系应该是多种解决不同问题的技术的有机组合。常见的配置有屏蔽路由器、



双宿主主机网关、屏蔽主机网关、屏蔽子网等。

防火墙在选购时应注意策略，如何选购一个安全、稳定、可靠的防火墙产品是非常重要的。

防火墙是目前用来实现网络安全措施的一种主要手段。

习　　题

一、填空题

1．常用的防火墙可以分为________和________两大类。

2．代理防火墙作用于________层。

3．双宿主主机网关中的双宿主主机是一台安装有________的计算机。

4．屏蔽主机网关由________和________组成。

5．屏蔽子网系统结构是在________基础上再加上一个屏蔽路由器构成。

二、选择题

1．防火墙自身有一些限制，它不能阻止________威胁。

I 外部攻击　　II 内部　　III 病毒感染

A．I　　B．I 和 II　　C．II 和 III　　D．全部

2．关于防火墙，以下说法错误的是________。

A．防火墙能隐藏内部 IP 地址

B．防火墙能控制进出内网的信息流向和信息包

C．防火墙能提供 VPN 功能

D．防火墙能阻止来自内部的威胁

3．________技术不是实现防火墙的主流技术。

A．包过滤技术　　B．应用级网关技术

C．代理服务器技术　　D．NAT 技术

4．防火墙采用的最简单的技术是________。

A．安装保护卡　　B．隔离　　C．包过滤　　D．设置进入密码

三、简答题

1．什么是防火墙？防火墙分为哪几类？

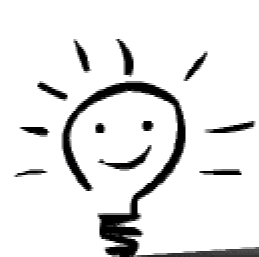
2．防火墙有哪些功能特点？

3．试述包过滤防火墙技术的原理及特点。

4．试述代理防火墙技术的原理及特点。

5．常见的防火墙体系结构有哪几种？

6．选购防火墙时应注意哪些问题？



本 章 实 训

实训 1　应用天网防火墙防范木马

实训目的

（1）了解防火墙的基本功能。

（2）掌握天网防火墙的使用，熟悉天网防火墙的配置规则。

实训环境

（1）一台连上 Internet 的计算机。

（2）最新天网防火墙个人版。

操作步骤

第 1 步：如果在天网防火墙运行时，木马服务器程序要打开网络端口，此时会弹出“天网防火墙警告信息”提示框，即可很容易检测到自己运行的程序是否被绑定了木马。

第 2 步：如果要想防止某程序使用网络资源，则单击“天网防火墙警告信息”提示框中的“禁止”按钮即可，这样攻击者就无法通过木马服务器程序来对被攻击者的机器进行远程控制了。而对于那些已经被植入木马到计算机中的用户，则可以采用如下的防御方法。

第 3 步：在天网防火墙主窗口中单击“增加规则”按钮，即可打开“增加 IP 规则”对话框，在 “规则”选项组的“名称”文本框中输入“禁止冰河木马的侵入”，在“说明”文本框中输入“记录冰河木马入侵，方法是记录 7626 端口的访问情况，在发现有冰河木马入侵的时候，同时发声”，在“数据包方向”下拉列表框中选择“接收”选项，再在“对方 IP 地址”下拉列表框中选择“任何地址”选项，如图 5.6 所示。

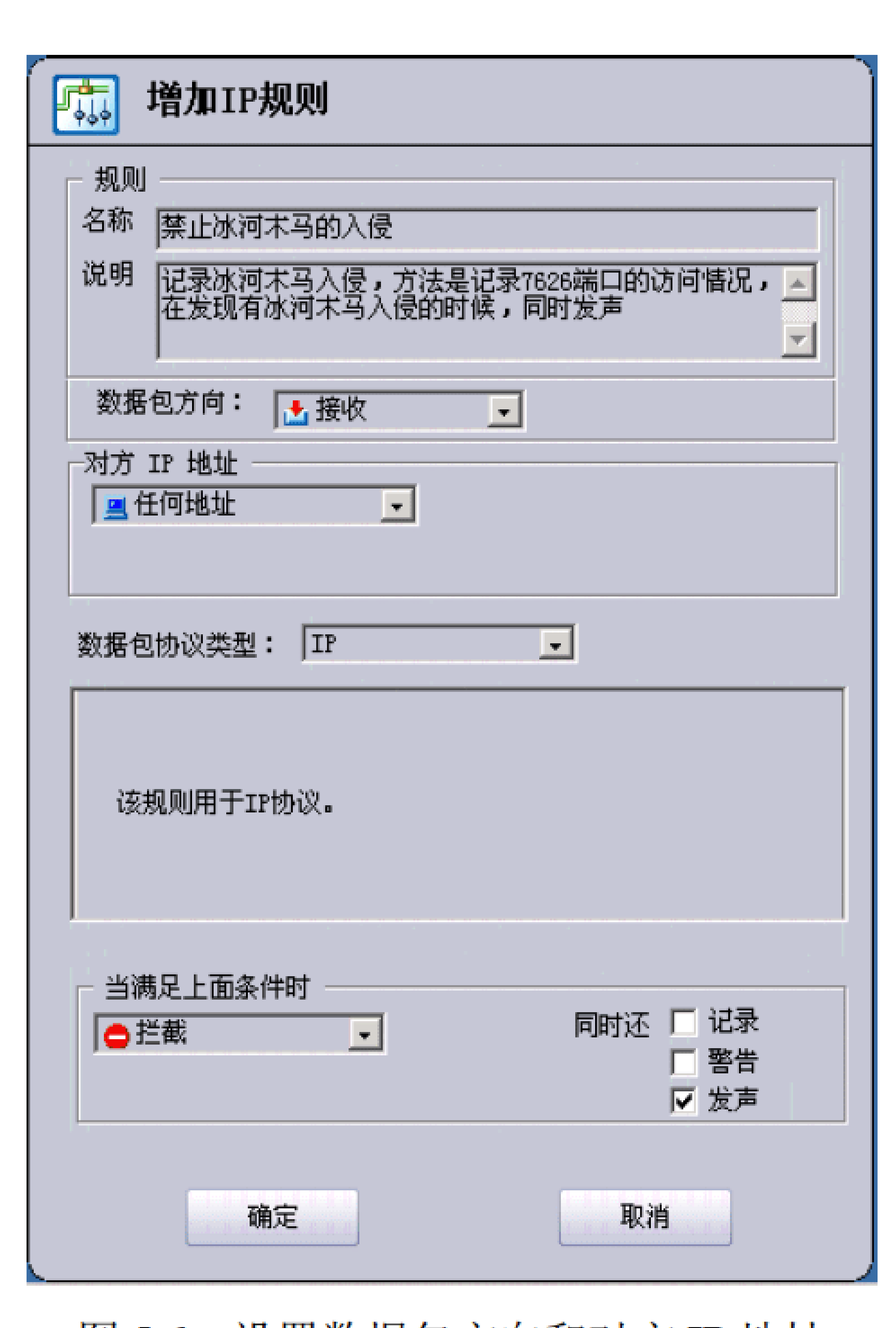


图 5.6　设置数据包方向和对方 IP 地址

图 5.7　TCP 类型

第 4 步：在“数据包协议类型”下拉列表框中选择 TCP 选项之后，将出现 TCP 类型框，在“本地端口”选项组中设定端口为从 7626 到 7626，如图 5.7 所示。在“数据包协议类型”下拉列表框中选择 UDP 项后，将出现 UDP 类型框，



在“本地端口”选项组中设定端口为从 7626 到 7626，如图 5.8 所示。

这两处（TCP/UDP）的设置主要是为了监听 7626 端口而进行的，因为冰河木马服务器程序就是使用这个端口与客户端程序进行通信的。

第 5 步：在“当满足上面条件时”下拉列表框中选择“通行”选项后，再在“同时还”选项组中选中“记录”和“发声”复选框，如图 5.9 所示。此时，在“自定义 IP 规则”列表框中就可以看到“禁止冰河木马的侵入”规则了，如图 5.10 所示。



图 5.8　UDP 类型

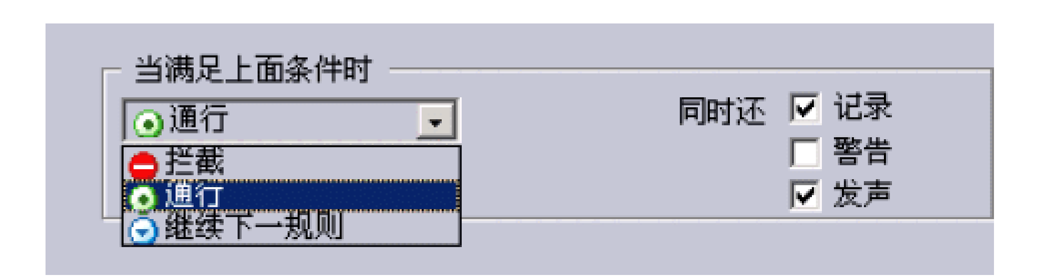


图 5.9　设置动作

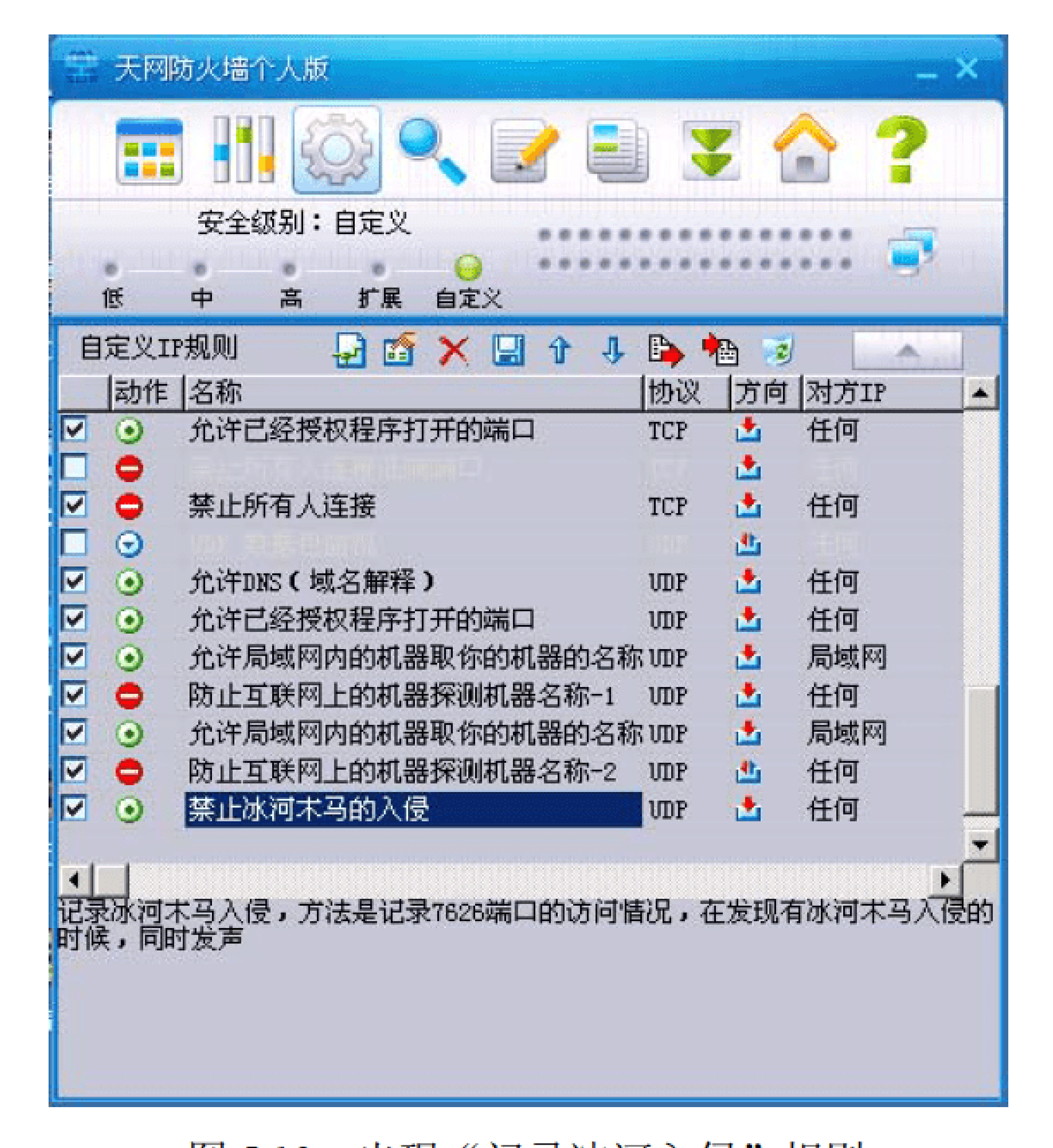


图 5.10　出现“记录冰河入侵”规则

经过上述设置之后，只要有其他计算机想通过冰河客户端程序控制本地计算机，本地计算机将在“天网防火墙”图标上出现“！”并不断闪烁，同时还发出警报声音。单击“日志”按钮后，天网防火墙可显示是哪些 IP 通过木马访问本地计算机的提示信息。

实训 2　应用天网防火墙打开 21 和 80 端口

实训目的

掌握天网防火墙的端口设置功能的使用。

实训环境

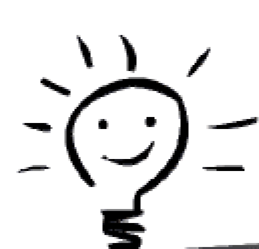
（1）一台连上 Internet 的计算机。

（2）最新天网防火墙个人版。

操作步骤

第 1 步：按图 5.11 所示设置打开 Web 服务 80 端口的 IP 规则。

第 2 步：单击“确定”按钮，并使其生效。



第 3 步： 按图 5.12 所示设置打开 FTP 服务 21 端口的 IP 规则。

第 4 步： 单击“确定”按钮，并使其生效。



图 5.11 打开 Web 服务 80 端口的 IP 规则



图 5.12 打开 FTP 服务 21 端口的 IP 规则

第6章 入侵检测技术

知识目标

- 了解入侵检测的概念、功能特点和安全性。
- 理解入侵检测系统的分类。
- 理解入侵检测系统的基本技术。

技能目标

- 熟悉常用入侵检测系统产品。
- 熟练使用常见入侵检测系统。
- 掌握入侵检测系统的选购、安装和维护方法。

随着网络安全问题的日益严峻，入侵检测系统凭借其自身特点有效地弥补了传统安全保护措施的不足，已成为计算机与网络安全的重要组成部分。

6.1 入侵检测简介

6.1.1 入侵检测

1. 入侵检测的概念

入侵检测（Intrusion Detection），顾名思义，是对入侵行为的检测，它通过对计算机网络或计算机系统中若干关键点收集信息并对其进行分析，从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。进行入侵检测的软件与硬件的组合便是入侵检测系统（Intrusion Detection System，IDS）。与其他安全产品不同的是，入侵检测系统需要更多的智能，它必须可以将得到的数据进行分析，并得出有用的结果。一个合格的入侵检测系统能大大简化管理员的工作，保证网络安全的运行。

假如防火墙是一幢大楼的门锁，则 IDS 就是这幢大楼里的监视系统。一旦小偷爬窗进入大楼，或内部人员有越界行为，只有实时监视系统才能发现情况并发出警告。入侵检测系统能够识别出任何不希望有的活动，这种活动可能来自于网络外部和内部。入侵检测系统的应用，能使在入侵攻击对系统发生危害前，检测到入侵攻击，并利用报警与防护系统驱逐入侵攻击；在入侵攻击过程中，能减少入侵攻击所造成的损失；在被入侵攻击后，收集入侵攻击的相关信息作为防范系统的知识，添加到知识库内，以增强系统的防范能力。

入侵检测系统处于防火墙之后对网络活动进行实时检测。许多情况下，由于可以记录和禁止网络活动，所以入侵检测系统是防火墙的延续。它们可以与防火墙和路由器配合工作。应当理解入侵检测系统是独立于防火墙工作的。

入侵检测系统 IDS 与系统扫描器 System Scanner 不同。系统扫描器是根据攻击特征数据库来扫描系统漏洞的，它更关注配置上的漏洞而不是当前进出你主机的流量。在遭受攻击的主机上，即使正在运行扫描程序，也无法识别这种攻击。

IDS 扫描当前网络的活动、监视和记录网络的流量，根据定义好的规则来过滤从主机网卡到网线上的流量，提供实时报警。网络扫描器检测主机上先前设置的漏洞，而 IDS 监视和记录网络流量。如果在同一台主机上运行 IDS 和扫描器的话，配置合理的 IDS 会发出许多报警。

2. 入侵检测的功能

（1）监视、分析用户和系统的行为。
（2）审计系统配置和漏洞。
（3）识别已知的攻击行为。
（4）评估系统关键资源和数据文件的完整性。
（5）统计分析异常行为。

（6）安装诱骗服务器，记录非法入侵行为。

（7）操作系统日志管理，并识别违反安全策略的用户活动。

3. 入侵检测系统的需求特性

（1）可靠性：检测系统必须在无人监控的情况下连续运行。系统必须是可靠的，这样才可以允许它运行在被检测的系统环境中。

（2）适应性：检测系统必须能随时追踪系统环境的改变。

（3）有效性：能检测系统的报告错误或漏报控制在一定的范围内。

（4）安全性：检测系统必须难以被欺骗，能够保护自身的安全。

（5）容错性： 检测系统的容错要求即使在系统崩溃的情况下，检测系统仍能保留下来。

6.1.2　入侵检测的发展

入侵检测系统需要实现的目标是发现网络上所有的异常行为与错误。近 20 多年来，入侵检测系统都是围绕着这个观念来发展的。但最近，对入侵检测系统的观点有了较大的转变，入侵检测系统逐渐普及并结合到其他的信息系统安全的各部分中。

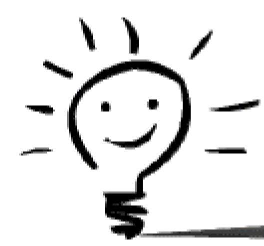
入侵检测系统的概念诞生于 1980 年，James Anderson 发表了文章 Computer Security Threat Monitoring and Surveillance，这篇文章介绍了对网络上用户的行为及信息进行审计的一种方法。随着文章的发表，“检测”这个概念逐渐被用户所接受。Anderson 对于入侵检测的理论成为入侵检测系统设计及开发的基础，他的工作成为基于主机的入侵检测系统和其他入侵检测系统的出发点。

在 1983 年，SRI 组织和 Dorothy 博士开始为一个政府项目而工作，将一些新的技术应用到入侵检测系统的开发当中。他们的目标是利用政府的大型计算机对用户的行为踪迹进行分析，然后在分析结果的基础上建立用户行为的轮廓模型。一年之后，Dorothy 博士帮助建立起了第一个入侵检测的模型：入侵检测专家系统（Intrusion Detection Expert System，IDES）。这项工作为入侵检测技术的发展提供了良好的基础并带动了入侵检测的发展。

1984 年，SRI 开发了一种方法来跟踪和分析包含 ARPANET 用户身份验证信息的审计数据。很快，SRI 在与海军的一份合同中首次实现了入侵检测系统。入侵检测系统使用的是 Dorothy 博士在 SRI 工作期间的研究成果。Dorothy 博士发表的这个有决定性的成果——入侵检测系统模型，为开发商业化入侵检测系统提供了必不可少的信息，他的文章成为入侵检测系统发展的基础。

1988 年，在美国空军一个名为“干草堆”的项目中，另一种版本的入侵检测系统也被实现了。这个项目的产品是一个通过分析审计数据并比较其中是否存在已定义的内容来工作的入侵检测系统。一位前“干草堆”项目的成员说：“在一大堆数据中查找是否有特点细节的行为就如同在干草堆中寻找一根针。”

在这之后，通过在网络中同时布置多个入侵检测系统协同工作的方式也诞生了，这种方式被称为分布式入侵检测系统（Distributed Intrusion Detection System，DIDS）。分布式入侵检测系统是原有入侵检测系统的扩展，这样通过跟踪客户机的方式比原来监视服务器的方式要好得多。最后，在 1989 年，“干草堆”项目发展形成了一个商业公司，“干草堆”实验室同时发布



使用新一代技术的产品 Stalker，Stalker 是一个基于网络的入侵检测系统。

进入 20 世纪 90 年代后，网络入侵检测系统的概念被提出。1990 年，Heberlein 作为最主要的开发者开发出了网络安全监视器（Network Security Monitor，NSM），这就是第一个网络入侵检测系统。这种新的方式引起了入侵检测行业以及风险投资的极大兴趣。Heberlein 的贡献甚至影响到了分布式入侵检测系统项目发展的方向，加入“干草堆”开发小组，他提出了第一个混合入侵检测系统的想法，他介绍的网络入侵检测系统引起了入侵检测行业的一次革命，并将“干草堆”项目带往了商业道路上。

入侵检测技术的商业化最早是在 1990 年初，“干草堆”实验室第一个推出了商业化的入侵检测工具——Stalker。Stalker 是一个标准的基于主机的入侵检测系统，而正在开发的 SAIC 则是另一种形式的入侵检测系统，称为计算机错误检测系统（Computer Misuse Detection System，CMDS）。同时，美国空军的密码技术中心也开发出一种审计安全衡量系统（Audit Security Measurement System，ASMS），用于监视美国空军网络传输数据。与其他的网络入侵检测系统相比，审计安全衡量系统的优势在于可测量性和便于携带。审计安全衡量系统也是第一个将硬件与软件结合的网络入侵检测解决方案，并被美国空军计算机安全紧急响应中心广泛应用在全世界各地。ASMS 项目的开发小组在 1994 年也发展成了一家商业公司——the Wheel Group，他们的产品 NetRanger，是第一个可用于商业化的网络入侵检测系统。

入侵检测市场逐渐扩大并开始带来收入是在 1997 年左右，在这一年，Cisco 公司认识到网络入侵检测的重要性并收购了 the Wheel Group，并开始向客户提供安全解决方案。同样，网络安全行业的领导者，ISS 公司也开发出了自己的网络入侵检测系统 RealSecure。一年后，第一个可视化基于主机入侵检测系统的公司（Centrax 的公司）与“干草堆”实验室合并。从此，入侵检测的世界逐渐被市场所主导。

由于入侵检测系统的市场在近几年中飞速发展，许多公司都投入到这一领域中来。除了国外的 ISS、Axent、NFR、Cisco 等公司外，国内也有数家公司（如中联绿盟、中科网威等）推出了自己相应的产品。但就目前而言，入侵检测系统还缺乏相应的标准。有两个组织试图对 IDS 进行标准化工作，即 IETF 的 IDWG（Intrusion Detection Working Group）和 CIDF（Common Intrusion Detection Framework），但其工作进展非常缓慢，目前尚没有被广泛接受的标准出台。

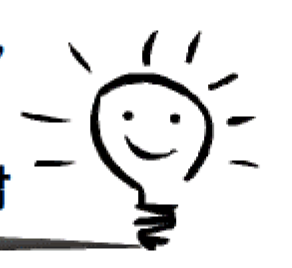
6.2　入侵检测系统

6.2.1　入侵检测系统的组成

从功能上讲，入侵检测系统由探测器（Sensor）、分析器（Analyzer）和用户接口（User Interface）组成。下面分别对这 3 个部分进行简要介绍。

1. 探测器

探测器主要负责收集数据。探测器的输入数据包括任何可能包含入侵行为线索的数据，



比如说网络数据包、日志文件和系统调用记录等。探测器将这些数据收集起来，然后发送到分析器进行处理。

2. 分析器

分析器又可称为检测引擎（Detection Engine），它负责从一个或多个探测器处接收信息，并通过分析来确定是否发生了非法入侵活动。分析器组件的输出是标识入侵行为是否发生的指示信号，例如一个警告信号，该指示信号中还可能包括相关的证据信息。另外，分析器组件还能够提供关于可能的反应措施的相关信息。

3. 用户接口

IDS 的用户接口使得用户易于观察系统的输出信息，并对系统行为进行控制。在某些系统中，用户接口又称为“管理器”、“控制器”或者“控制台”等。

除了以上 3 个必要组件外，某些 IDS 可能还包括一个所谓的“蜜罐”（Honeypot）诱饵机。该诱饵机被设计和配置成具有明显的系统安全漏洞，并对攻击者明显可见。诱饵机能够作为 IDS 中一个专门提供给攻击者进行入侵的探测器来使用，从而提供关于某次攻击行为的发生过程和相关信息。

6.2.2　入侵检测系统的类型

从技术上看，入侵检测系统可以分为基于主机的入侵检测、基于网络的入侵检测、混合入侵检测和网络节点的入侵检测等。

1. 基于主机的入侵检测

基于主机的入侵检测（Host-based Intrusion Detection，HID）是被设计用于监视、检测对于主机的攻击行为，通知用户并进行响应。有些功能强大的工具甚至能提供审计策略管理与集中控制，提供数据对比、统计与分析支持。

基于主机的入侵检测设备通常是安装在被重点检测的主机之上，其目标主要是主机系统和本地用户，主要是对该主机的网络实时连接以及对系统审计日志进行智能分析和判断。如果其中主体活动十分可疑（特征或违反统计规律），入侵检测系统就会采取相应的措施。基于主机的入侵检测系统的结构如图 6.1 所示。

图 6.1　基于主机的入侵检测系统

基于主机的入侵检测系统的优点如下。

（1）基于主机的入侵检测系统对分析可能的攻击行为非常有用。举例来说，有时候它除了指出入侵者试图执行的一些“危险的命



令”外，还能分辨入侵者干了什么事，他们运行了什么程序、打开了哪些文件、执行了哪些系统调用。主机入侵检测系统与网络入侵检测系统相比通常能够提供更详尽的相关信息。

（2）主机入侵检测系统通常情况下比网络入侵检测系统误报率要低，因为检测在主机上运行的命令序列比检测网络流更简单，系统的复杂性也少得多。

（3）主机入侵检测系统可安装在那些不需要广泛的入侵检测、传感器与控制台之间的通信带宽不足的情况下。主机入侵检测系统在不使用诸如“停止服务”、“注销用户”等响应方法时风险较少。

基于主机的入侵检测系统的缺点如下。

（1）主机入侵检测系统安装在需要保护的设备上。例如，当一个数据库服务需要保护时，就要在服务器本身上安装入侵检测系统。这会降低应用系统的效率。

（2）主机入侵检测系统依赖于服务器固有的日志与监视能力。如果服务器没有配置日志功能，则必须重新配置，这将会给运行中的业务系统带来不可预见的性能影响。

（3）全面安装主机入侵检测系统代价较大，企业中很难将所有主机用主机入侵检测系统保护，只能选择分主机保护。那些未安装主机入侵检测系统的机器将成为保护的盲点，入侵者可利用这些机器攻击目标。

（4）主机入侵检测系统除了监测自身的主机以外，根本不监测网络上的情况。对入侵行为分析的工作量将随着主机数目增加而增加。

2. 基于网络的入侵检测

基于网络的入侵检测（Network Intrusion Detection，NID）是通过分析主机之间网络上传输的信息来工作的。网络入侵检测设备能截取利用不同传输介质以及不同协议进行传输的数据包（大部分入侵检测系统主要是针对 TCP/IP 协议）。

基于网络的入侵检测设备（NIDS）放置在比较重要的网段内，不停地监视网段中的各种数据包，对每一个数据包或可疑的数据包进行特征分析。如果数据包与产品内置的某些规则吻合，入侵检测系统就会发出警报甚至直接切断网络连接。目前，大部分入侵检测产品是基于网络的。基于网络的入侵检测系统是根据网络流量、网络数据包和协议来分析检测入侵行为的，基本过程如图 6.2 所示。

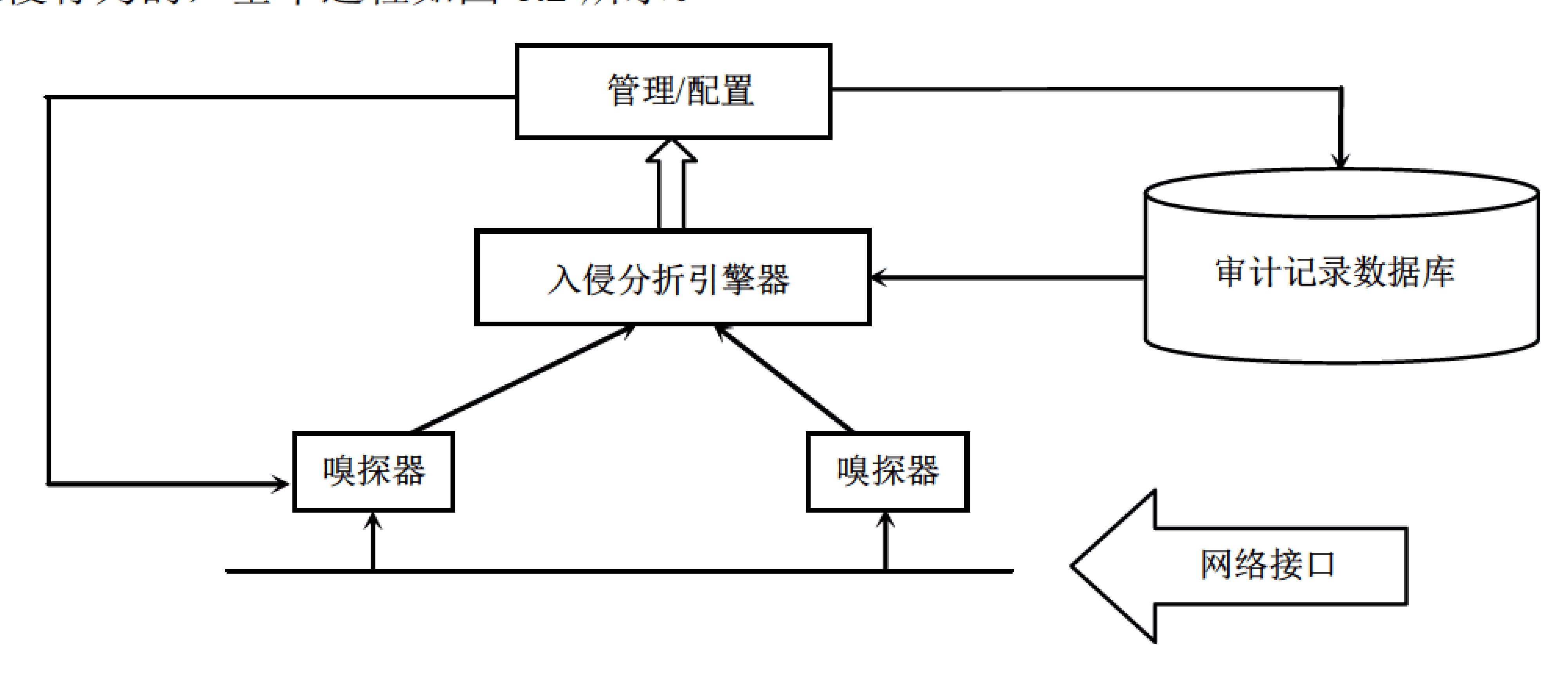


图 6.2　基于网络的入侵检测系统



基于网络的入侵检测系统的优点如下。

（1）网络入侵检测系统能够检测那些来自网络的攻击，它能够检测到超过授权的非法访问。

（2）一个网络入侵检测系统不需要改变服务器等主机的配置。由于它不会在业务系统的主机中安装额外的软件，从而不会影响这些机器的 CPU、I/O 与磁盘等资源的使用，不会影响业务系统的性能。

（3）由于网络入侵检测系统不像路由器、防火墙等关键设备那样工作，所以它不会成为系统中的关键路径。网络入侵检测系统发生故障不会影响正常业务的运行。安装网络入侵检测系统的风险比安装主机入侵检测系统的风险小得多。

（4）网络入侵检测系统近几年有向专门的设备发展的趋势，安装这样的一个网络入侵检测系统非常方便，只需将定制的设备接上电源，做很少的配置，将其连到网络上即可。

基于网络的入侵检测系统的缺点如下。

（1）网络入侵检测系统只检测它直接连接网段的通信，不能检测在不同网段的网络包。在使用交换以太网的环境中会出现检测范围的局限。而安装多台网络入侵检测系统的传感器会使整个系统的成本大大增加。

（2）网络入侵检测系统为了性能目标通常采用特征检测的方法，它可以检测出普通的一些攻击，而很难实现一些复杂的、需要大量计算与分析时间的攻击检测。

（3）网络入侵检测系统可能会将大量的数据传回分析系统中。在一些系统中监听特定的数据包会产生大量的分析数据流量。一些系统在实现时采用一定方法来减少回传的数据量，对入侵判断的决策由传感器实现，而中央控制台成为状态显示与通信中心，不再作为入侵行为分析器。这样的系统中的传感器协同工作能力较弱。

（4）网络入侵检测系统处理加密的会话过程较困难，目前通过加密通道的攻击尚不多，但随着 IPv6 的普及，这个问题会越来越突出。

随着网络系统结构复杂化和大型化，出现了许多基于分布式的入侵检测。例如：

（1）系统的弱点或漏洞分散在网络中的各个主机上，这些弱点可能被入侵者一起用来攻击网络，而依靠唯一的主机或网络 IDS 不能发现入侵行为。

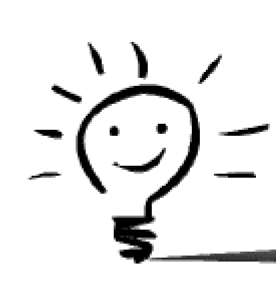
（2）入侵行为不再是单一的行为，而是表现出相互协作的入侵特点，如分布式拒绝服务攻击（DDoS）。

（3）入侵检测所依靠的数据来源分散化，收集原始的检测数据变得困难，如交换型网络使得监听网络数据包受到限制。

（4）网络速度传输加快，网络的流量大，集中处理原始数据的方式往往造成检测瓶颈，从而导致漏检。

基于这样的情况，分布式入侵检测系统就应运而生。

分布式 IDS 通常由数据采集构件、通信传输构件、入侵检测分析构件、应急处理构件和管理构件组成，如图 6.3 所示，这些构件可根据不同情形进行组合。



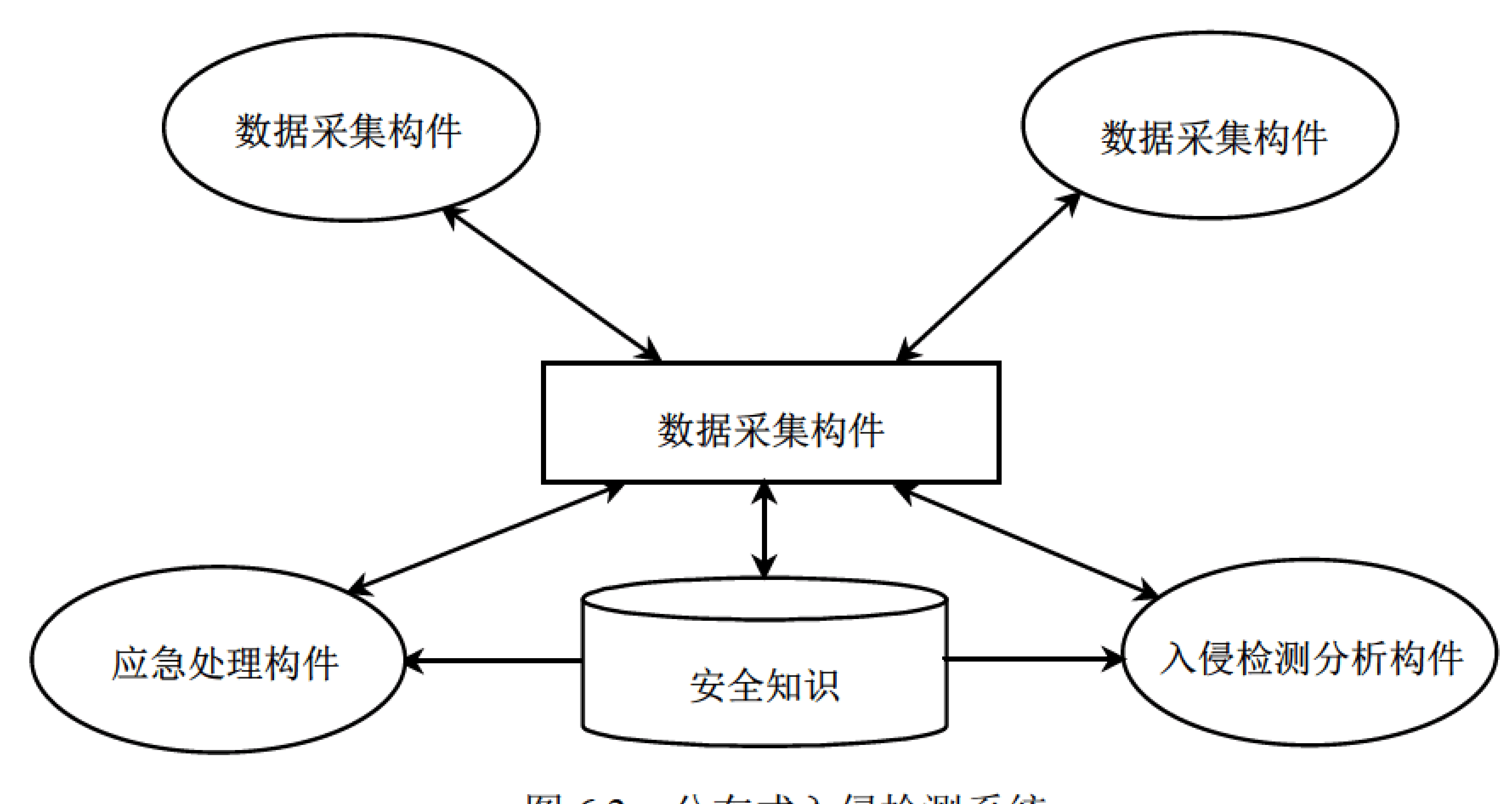


图 6.3　分布式入侵检测系统

3. 混合入侵检测

混合入侵检测系统是基于网络和基于主机的入侵检测系统的结合，这种混合的解决方案为 NID 和 HID 提供了互补，并提供了入侵检测的集中管理。采用这种技术能实现对入侵行为的全方位检测，避免入侵行为被忽略掉。

4. 网络节点的入侵检测

网络节点入侵检测（Network-Node Intrusion Detection，NNID）是为加固传统的网络入侵检测周围环境而开发的，它使用 sniffer 技术截取从网线上传输给主机的数据包。与网络入侵检测不同的是，网络节点入侵检测是在数据包到达主机后进行截取。网络节点入侵检测的设想来源于多个 HID 中心理论，即每一个中心主机都必须利用基于主机的技术优势。通常网络节点入侵检测只是简单地附在主机入侵检测上的一个模块上。

由于嗅探技术的限制，网络节点入侵检测仅仅能分析目的地址是主机地址的包，但是由于网络节点入侵检测的特性，当网络使用的是一个高速通信网络、加密网络或者使用了交换式设备时，网络节点入侵检测仍然能对所有的子网进行检测。网络节点入侵检测的优势在于，能有效的抵御针对特定主机的基于包的攻击。

6.3　常用的入侵检测方法

对于收集到的有关系统、网络、数据及用户活动的状态和行为等信息，一般通过 3 种技术手段进行分析：模式匹配、统计分析和完整性分析。前两种方法用于实时的入侵检测，而完整性分析则用于事后分析。

1. 模式匹配

模式匹配就是将收集到的信息与已知的网络入侵和系统误用模式数据库进行比较，从而发现违背安全策略的行为。该过程可以很简单（如通过字符串匹配以寻找一个简单的条



目或指令)，也可以很复杂（如利用正规的数学表达式来表示安全状态的变化)。一般来讲，一种进攻模式可以用一个过程（如执行一条指令）或一个输出（如获得一个权限）来表示。该方法的一大优点是只需收集相关的数据集合，显著减少系统负担，且技术已相当成熟。它与病毒防火墙采用的方法一样，检测准确率和效率都相当高。但是，该方法存在的弱点是需要不断的升级以对付不断出现的黑客攻击手法，不能检测到从未出现过的黑客攻击手段。

2. 统计分析

统计分析方法首先给系统对象（如用户、文件、目录和设备等）创建一个统计描述，统计正常使用的一些测量属性（如访问次数、操作失败次数和延时等)。测量属性的平均值将被用来与网络、系统的行为进行比较，任何观察值在正常范围之外时，就认为有入侵发生。例如，统计分析可能标识一个不正常行为，因为它发现一个在晚八点至早六点不登录的账户却在凌晨两点试图登录。其优点是可检测到未知的入侵和更为复杂的入侵，缺点是误报、漏报率高，且不适应用户正常行为的突然改变。具体的统计分析方法如基于专家系统的、基于模型推理和基于神经网络的分析方法，目前正处于研究热点和迅速发展之中。

3. 完整性分析

完整性分析主要关注某个文件或对象是否被更改，这经常包括文件和目录的内容及属性，它在发现被更改的、被木马化的应用程序方面特别有效。完整性分析利用强有力的加密机制，称为消息摘要函数（如 MD5)，它能识别哪怕是很微小的变化。其优点是不管模式匹配方法和统计分析方法能否发现入侵，只要是成功的攻击导致了文件或其他对象的任何改变，它都能够发现。缺点是一般以批处理方式实现，不用于实时响应。尽管如此，完整性检测方法还应该是网络安全产品的必要手段之一。例如，可以在每一天的某个特定时间开启完整性分析模块，对网络系统进行全面地扫描检查。

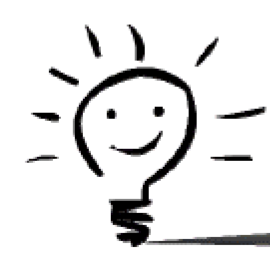
6.4 入侵检测系统的未来发展

6.4.1 入侵检测系统的局限性

入侵检测系统也面临着若干重要的挑战。这些挑战有些来自技术方面，有些则来自非技术方面。

1. 技术方面的主要挑战

（1）网络规模和复杂程序的不断增长。在一个大型的异构网络环境中，入侵检测系统所遇到的主要问题包括如何集成并处理来自分布在网络各处实体的具有不同格式的各种相关信息、如何在相互合作但是并不完全相互信任的组织之间来共享敏感的相关入侵行为信



息、如何进行管理域间的合作进程以及如何保证在局部入侵检测系统失效的情况下仍能维护系统全局的安全等。

（2）预警技术。是指如何在造成损失前及早发现入侵活动。

（3）网络繁忙情况下的系统性能问题。为了保证发挥效能，网络入侵检测系统必须能够分析所有的内向数据包。如果一个入侵检测系统无法应付网络吞吐量的话，它就可能漏掉不少反映入侵活动的特征数据，从而造成安全漏洞。

（4）入侵模式特征的准确性。用来描述异常入侵行为的模式特征是滥用检测系统最重要的基石。如何保证所采用的特征集能够准确而又足以描述已知的各种攻击模式（包括复杂的分阶段攻击行为）及其变种，是一个重要而敏感的问题。

（5）入侵检测系统的评估。对入侵检测系统评估测试是一项复杂的工作，因为 IDS 不能在独立环境中检测，首先必须建立一个实际网络平台环境。同时，还需要大量的包含各种测试入侵的复杂数据，这些数据还要根据不同的操作系统平台和版本加以调整。时至今日，在这方面所做的工作非常少。

2. 非技术因素

（1）攻击者不断研究新的攻击模式，同时，随着安全技术的普及，越来越多的人进行了越来越多的入侵攻击尝试。自动攻击的软件工具不断得到改进，使普通用户也能够利用它来进行网络攻击。各种机构（包括政府、公司等）对包括 IDS 在内的安全技术的认识不足或者缺乏足够经验的安全管理员。

（2）我国计算机系统及网络产品以国外的为主，软硬件系统中难免也存在各种潜在威胁和安全“陷阱”（如操作系统后门、路由器漏洞等）。因此，利用这些设备建立的网络系统，在其安全性方面得不到根本性的保障。

6.4.2 入侵检测的未来发展

入侵检测系统与其他的网络产品一样，在过去几年获得了非常大的发展，其已经成为维护网络安全的重要产品，就如同防火墙一样。不过，未来是很难预料的，网络的情况会改变，入侵者也在不断地学习。入侵检测系统必须要面对这些问题，并不断地演化以适应环境的变化。无论如何，管理员都必须确信入侵检测系统是帮助他们维护网络安全最有力的武器之一。下面几方面是未来对入侵检测发展可能带来影响的因素。

1. 安全事件逐年上升

对管理员而言，将网络接入到互联网中，就意味着将网络暴露在全球的入侵者面前，大量的攻击行为将使入侵检测系统面临更大的压力。

2. 安全问题日渐增多

互联网不断发展使得网络日趋复杂，软件的功能不断增加，然而安全漏洞被发现的数量也不断扩大。除了操作系统外，各种服务软件的漏洞都有可能给系统带来安全方面的威胁。入侵检测系统必须具备足够的能力跟踪最新的漏洞出现。



3. 良好的适应性

网络入侵检测系统通过匹配网络数据包发现攻击行为，入侵检测系统往往假设攻击信息是通过明文传输的，因此对信息稍加改变便可能骗过入侵检测系统的检测。一些攻击者已经开始利用这一点通过加密的方法传输控制信息。还有许多系统通过 VPN（虚拟专用网）进行网络之间的互联，如果入侵检测系统不了解其所用的隧道机制，就会无法发现可能存在的入侵行为。

4. 必须协调、适应多样性的环境中的不同的安全策略

网络及其中的设备越来越多样化，既存在关键资源如邮件服务器、企业数据库，也存在很多相对不是很重要的 PC 机，不同企业之间这种情况也往往不尽相同，入侵检测系统要能适应多样的环境要求。

6.5　入侵检测系统的选购策略

目前基于网络的入侵检测产品有很多，如果不考虑费用问题，可以使用优秀的商业产品，使用这些产品会得到来自开发商的技术支持和产品更新。当然还有很多的非商业化的产品，如 Snort 这一类的自由软件。选购产品最重要的就是量力而行，不要因为产品的名气而购买，记住你需要的是适合自己网络使用的入侵检测产品。

当选择入侵检测系统时，要从如下方面进行考虑。

（1）系统的价格。价格是必须考虑的要点，不过，性能价格比以及要保护系统的价值则是更重要的因素。

（2）特征库升级与维护的费用。像反病毒软件一样，入侵检测的特征库需要不断更新才能检测出新出现的攻击方法。

（3）对于网络入侵检测系统，最大可处理流量是多少包/秒（pps）。首先，要分析网络入侵检测系统所安装的网络环境，如果在 512Kbps 或 24Mbps 专线上安装网络入侵检测系统，则不需要高速的入侵检测引擎，而在负荷较高的环境中，性能是一个非常重要的指标。

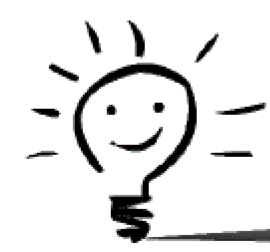
（4）该产品是否容易被躲避。常用的躲开入侵检测的方法包括分片、TTL 欺骗、异常 TCP 分段、慢扫描、协同攻击等。

（5）产品的可伸缩性。包括系统支持的传感器数目、最大数据库大小、传感器与控制台之间的通信带宽和对审计日志溢出的处理。

（6）运行与维护系统的开销。包括产品报表结构、处理误报的方便程度、事件与日志查询的方便程序以及使用该系统所需的技术人员数量。

（7）产品支持的入侵特征数。不同厂商对检测特征库大小的计算方法都不一样。

（8）产品有哪些响应方法。要从本地、远程等多个角度考察。自动更改防火墙配置是一个听起来很不错的功能，但是，自动配置防火墙是一个极为危险的举动。



（9）是否通过了国家权威机构的评测。主要的权威测评机构包括国家信息安全测评认证中心和公安部计算机信息系统安全产品质量监督检验中心。

理想的入侵检测系统方案应该具有以下几个特点。

（1）快速控制台。

（2）良好的误警报管理。

（3）显示已经分析过的事件。

（4）标志已经分析过的事件。

（5）层层探究的能力。

（6）关联分析能力。

（7）报告能力。

从目前的情况来看，每天都会有许多新的入侵方式出现，对于入侵事件的检测仅靠入侵检测系统是不现实的，但是也不能完全放弃入侵检测系统。即使是训练有素的专家级分析员也需要通过各种工具才能对这些入侵行为进行分析。一般来说，提供给分析员的信息越多，分析员解决入侵检测问题的机会就越大，但是任何事情都不能走入极端，过多的信息也有可能使分析员在大量的信息中迷失，将宝贵的时间和精力浪费在如何分离大量的无效信息上。因此合理的选择并部署入侵检测系统才能获得最合理的入侵检测能力。

6.6　入侵检测系统实例

6.6.1　常见入侵检测系统介绍

1. BlackICE

该软件在 1999 年获得了 PC Magazine 的技术卓越大奖，专家对它的评语是：“对于没有防火墙的家庭用户来说，BlackICE 是一道不可缺少的防线；而对于企业网络，它又增加了一层保护措施。它并不是要取代防火墙，而是阻止企图穿过防火墙的入侵者。BlackICE 集成有非常强大的检测和分析引擎，可以识别 200 多种入侵技巧，给你全面的网络检测以及系统防护，它还能即时监测网络端口和协议，拦截所有可疑的网络入侵，无论黑客如何费尽心机也无法危害到你的系统。而且它还可以将查明的那些试图入侵的黑客的 NetBIOS（WINS）名、DNS 名或是它目前所使用的 IP 地址记录下来，以便你采取进一步行动。该软件的灵敏度和准确率非常高，稳定性也相当出色，系统资源占用率极少，是每一位网络用户网络监测的最佳选择。”

BlackICE 的功能如下：

（1）在设置中增加了应用程序与通信控制的功能条。

（2）可控制应用程序是否在计算机上执行。

（3）可控制哪些应用程序能与 Internet 通信。



（4）扫描系统，检测所有系统的设置改变。

（5）可在事件列表中记录新软件与新通信事件的发生情况。

2. OSSEC HIDS

这一个基于主机的开源入侵检测系统，可以执行日志分析、完整性检查、Windows 注册表监视、rootkit 检测、实时警告以及动态的实时响应。除了其 IDS 的功能外，它通常还可以被用作一个 SEM/SIM 解决方案。因为其强大的日志分析引擎，互联网供应商、大学和数据中心都乐意运行 OSSEC HIDS，以监视和分析其防火墙、IDS、Web 服务器和身份验证日志。

6.6.2　入侵检测系统 Snort 简介

Snort 是一个免费的 IDS（入侵监测系统）软件，它的一些源代码是从著名的 TcpDump 软件发展而来的。它是一个基于 libpcap 包的网络监控软件，可以作为一个十分有效的网络入侵监测系统。

Snort 首先根据远端的 IP 地址建立目录，然后将检测到的包以 TcpDump 的二进制格式记录或者以自身的解码形式存储到这些目录中。这样一来，就可以使用 snort 来监测或过滤用户所需要的包。

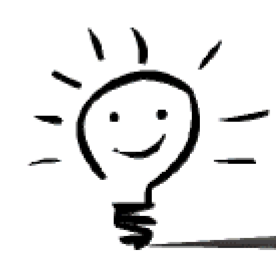
Snort 是一个轻量级的入侵检测系统，它具有截取网络数据报文，进行网络数据实时分析、报警，以及日志的能力。Snort 的报文截取代码是基于 libpcap 库的，继承了 libpcap 库的平台兼容性。它能够进行协议分析，内容搜索/匹配，能够用来检测各种攻击和探测，例如：缓冲区溢出、隐秘端口扫描、CGI 攻击、SMB 探测、OS 指纹特征检测等。Snort 使用一种灵活的规则语言来描述网络数据报文，因此可以对新的攻击做出快速地翻译。Snort 具有实时报警能力。可以将报警信息写到 syslog、指定的文件、UNIX 套接字或者使用 WinPopup 消息。Snort 具有良好的扩展能力，它支持插件体系，可以通过其定义的接口，很方便地加入新的功能。Snort 还能够记录网络数据，其日志文件可以是 TcpDump 格式，也可以是解码的 ASCII 格式。

简单地说，Snort 是数据包的嗅探器，也是数据包记录器，还是网络入侵检测系统（NIDS）。提供数据包嗅探和记录功能只是 Snort 的部分功能，Snort 的特点就是其入侵检测功能——根据入侵规则匹配数据包中的内容。

Snort 对硬件没有特殊的要求。对 Snort 来说，硬件系统的处理器频率越高越好，不同网络使用的网卡和硬盘空间大小会制约 Snort 捕捉数据包和存储数据包的功能。

Snort 的产品定位为简单 NIDS。现在能运行在 x86 平台的 Linux、FreeBSD、NetBSD、OpenBSD 和 Windows 等操作系统上。另外，Sparc Solaris、PowerPc、MacOS X、MKLinux 和 PA-RISC、HP-UX 等操作系统也都支持 Snort，可以说 Snort 可以在任何流行的平台上运行。

Snort 可提供 Protocol 分析、内容查找和匹配，可以用来检测各种攻击和探测，如缓冲区溢出、隐蔽端口扫描、CGI 攻击、SMB 探测、操作系统指纹识别尝试等。其中包嗅探、



数据包记录和入侵检测是其重要功能。Snort 的架构决定了它的各种功能，Snort 架构由以下 4 个基本模块构成。

（1）嗅探器。

（2）预处理器。

（3）检测引擎。

（4）输出模块。

Snort 的最简单形式就是包嗅探器，但当 Snort 获取到数据包后会将数据包传送到处理模块，然后通过检测引擎判断这些数据包是否违反了某些预定义规则。

Snort 的预处理器、检测引擎和输出模块都以插件形式存在。插件就是符合 Snort 接口定义的程序，这些程序曾经是 Snort 内核代码的一部分，现在独立出来使内核部分的修改变得简单可靠。

包嗅探器用来监听数据，可以是硬件也可以是软件。一个网络嗅探器使应用程序或者硬件设备能够监听网络上的数据流。互联网多是 IP 数据流，在本地局域网或传统网络中多是 IPX 或 AppleTalk 数据流。具体来说，包嗅探器可以进行网络分析及错误处理、性能分析及基准测量、监听明文密码及其他感兴趣的数据。

预处理器得到原始数据包，使用不同的插件检测数据包，这些插件检测数据包的某些特定行为。一旦数据包被确认具有某些特定行为，就会被送到检测模块。插件可以根据需要在与处理层被启用或停用，从而更具网络优化级被分配计算资源并生成报警，插件是入侵检测系统的一个非常有用的工具。

检测引擎接收预处理器及其插件传送来的数据，然后根据一系列的规则对数据进行检测。如果这些规则和数据包中的数据相匹配，就将数据包传送给报警处理器。

当数据通过检测引擎后，Snort 会对其数据进行不同的处理。如果数据和检测引擎的规则相匹配，Snort 就会触发报警。报警可以通过网络连接、UNIX 的套接字或 Windows Popup（SMB），甚至 SNMP 陷阱机制发送到日志文件。也可以使用 Snort 的一些附加工具来通过 Web 接口显示日志内容，包括一些 Perl、PHP 和 Web 服务器的插件等。日志可以存储在文本文件中。报警和日志都可以记录到数据库中，如 MySQL 或 Postgree 等。另外，Snort 报警可以通过系统日志工具如 SWATCH 发送电子邮件及时通知系统管理员，该系统不需要由专人 24 小时监控。

本 章 小 结

入侵检测系统是网络安全保障体系结构中的重要环节，它为实时安全事件审计、发现攻击者的入侵行为、采取及时的响应措施、避免系统受到进一步的危害提供了技术保障。

从功能上讲，入侵检测系统由探测器、分析器和用户接口组成。

入侵检测系统的数据可以来自多方面，针对这些安全审计数据源，入侵检测系统可以采取模式匹配、统计分析等误用检测或异常检测技术，对入侵行为做出及时的判断，帮助系统管理员更好地维护系统安全。

习　　题

一、填空题

1．入侵检测系统是________的系统。

2．入侵检测系统的需求特性有________性、________性、________性、________性和________性。

3．从功能上讲，入侵检测系统由________、________和________3 部分组成。

4．网络入侵检测是通过分析________来工作的。

5．混合入侵检测系统是________和________入侵检测系统的结合。

二、选择题

1．入侵检测利用的信息分析包括________。

A．系统和网络日志文件

B．目录和文件中的不期望的改变和程序执行中的不期望的行为

C．物理形式的入侵信息

D．以上所有信息

2．用于事后分析的入侵检测方法是________。

A．模式匹配　　B．统计分析

C．完整性分析　　D．可靠性分析

3．一个基于网络的入侵检测程序用________去检测攻击。

A．一次攻击的分析　　B．DNS 的配置

C．特征数据库　　D．包探测器

4．一个基于网络的入侵检测程序最适合检测________。

A．直接攻击和木马攻击　　B．直接攻击和拒绝服务攻击

C．端口扫描和拒绝服务攻击　　D．拒绝服务攻击和木马攻击

5．一个基于网络的入侵检测程序探测离开网络的数据包，系统的______最重要。

A．网卡的质量　　B．系统的制造商

C．系统的显示器　　D．内存的质量

三、简答题

1．入侵检测系统的作用有哪些？

2．入侵检测系统由哪些部分组成？

3．简述入侵检测系统发展的动态和趋势。

4．如何选购入侵检测系统？



本 章 实 训

实训　入侵检测软件 BlackICE 的使用

实训目的

（1）了解入侵检测技术的基本原理。

（2）掌握入侵检测工具 BlackICE 的使用。

实训环境

（1）一台连上 Internet 的计算机。

（2）入侵检测软件 BlackICE。

操作步骤

第 1 步：BlackICE 软件的下载安装。

可以在如华军软件园等网站下载，本实训以 BlackICE PC Protection 3.6 为例。下载、解压软件后，运行安装程序即可安装 BlackICE。

第 2 步：熟悉 BlackICE 软件界面。

BlackICE 软件界面如图 6.4 所示。

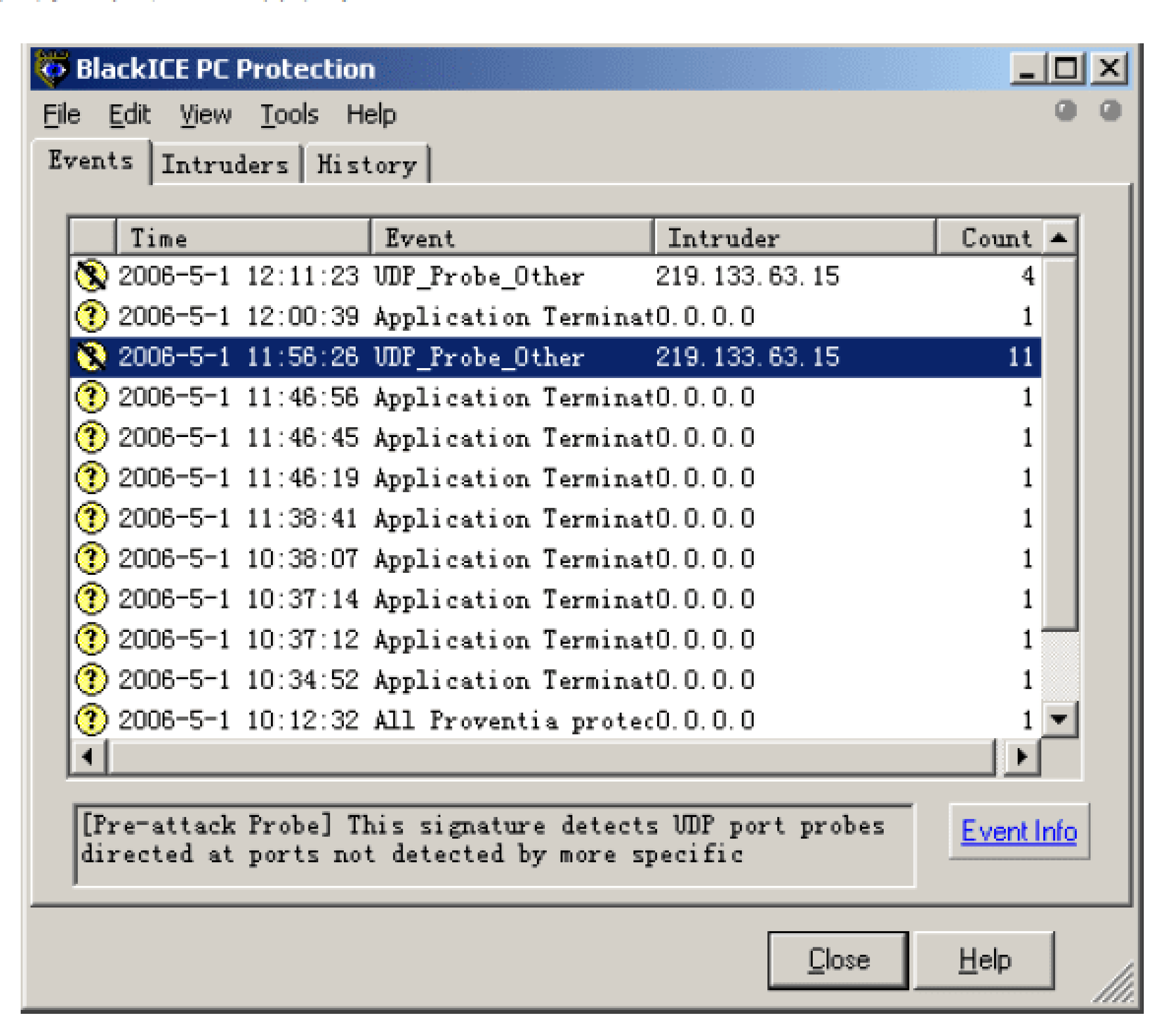


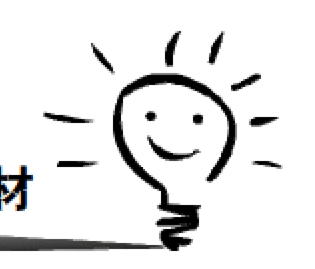
图 6.4　BlackICE 界面

（1）掌握菜单栏中菜单的操作内容。

（2）掌握 Events（事件）、Intruders（入侵）和 History（历史）3 个选项卡中的信息内容。

第 3 步：规则设置。

（1）规则设置与编辑。选择菜单栏中的 Tools（工具）→Edit BlackICE Settings（编辑 BlackICE 设置）命令，出现 BlackICE Settings 对话框，用户可以根据自己的需要进行配置。



（2）防火墙规则设置。选择菜单栏中的 Tools（工具）→Advanced Application Protection Settings（高级防火墙设置）命令，出现 Advanced Application Protection Settings（高级防火墙）对话框，如图 6.5 所示。根据需要可以添加、删除和修改防火墙项目。

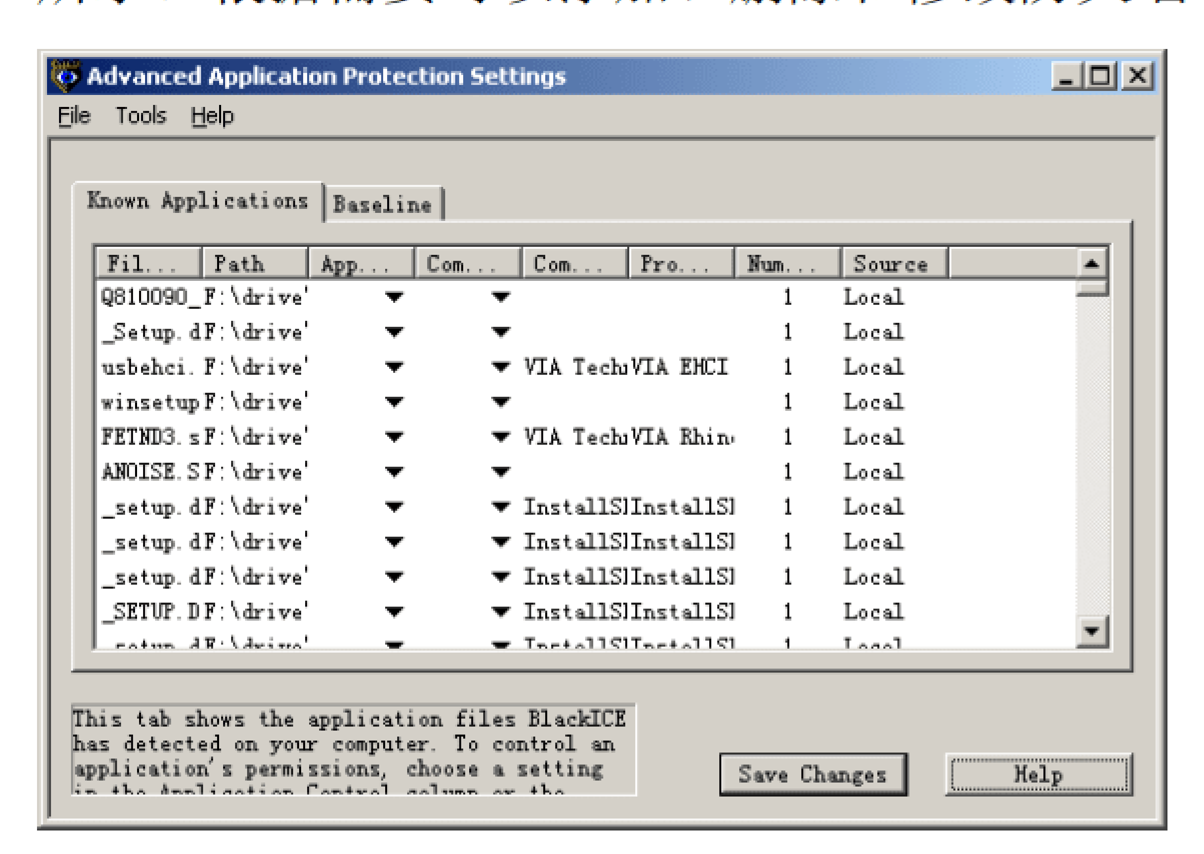


图 6.5　Advanced Application Protection Settings（高级防火墙）对话框

（3）查阅 Intruders（入侵者）信息，如图 6.6 所示。其中可以直接将入侵者的 IP 地址、计算机名、NetBIOS 名、DNS 名、MAC 地址等显示出来。如果用户确认某入侵者后，可以在入侵者上单击鼠标右键，在弹出的快捷菜单中通过选择 Block Intruders（拦截入侵者）选项可以设置拦截入侵者的时间，时间共有 4 个选项：For an Hour（1 小时）、For a Day（1 天）、For a Month（1 个月）和 Forever（永久）。

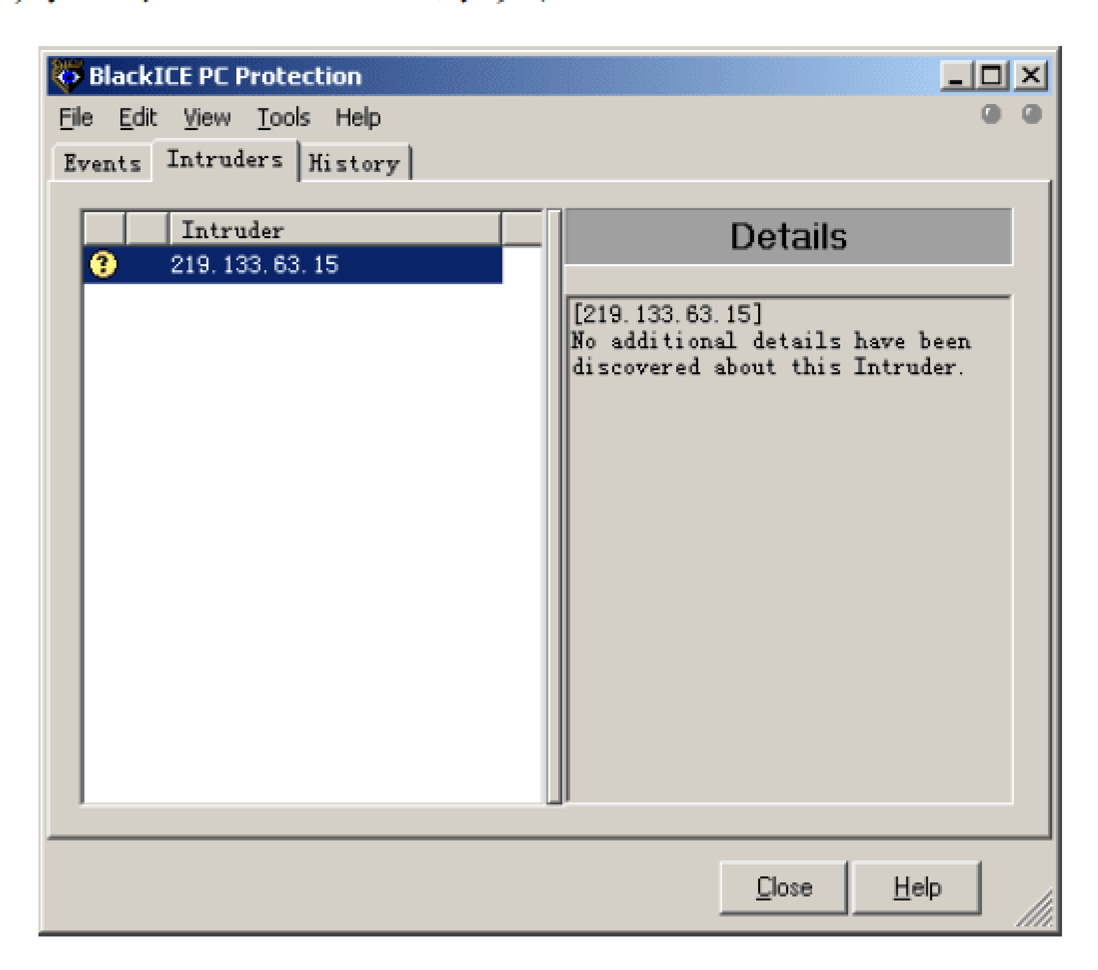


图 6.6　Intruders（入侵者）标签设置界面

第 7 章

网络病毒安全

知识目标

- 熟悉计算机病毒的定义、分类、特点。
- 了解网络病毒的特点、传播方式。
- 熟悉常用杀毒软件的功能。

技能目标

- 熟悉网络病毒的清除方法与过程。
- 熟练掌握常用杀毒软件的使用。

随着计算机网络的快速发展以及网络应用的不断深入，计算机病毒的防治显得更加重要。Internet 时代，网络成为了计算机病毒最好的传播途径。病毒扩散速度之快也是前所未有的，严重威胁着网络的安全。

7.1　计算机病毒概述

7.1.1　计算机病毒的定义

从广义上定义，凡能引起计算机故障、破坏计算机数据的程序统称为计算机病毒。“计算机病毒”的概念是由美国计算机研究专家 F.Cohen 最早提出来的，像生物病毒一样，计算机病毒具有独特的复制能力。它们能把自身附在各种类型的文件上，当文件被复制或从一个用户传送到另一个用户时，它们就随同文件一起蔓延开来。除复制能力外，某些计算机病毒还有其他一些共同特性：一个被感染的程序能够传送病毒载体。当你看到病毒载体似乎仅仅表现在文字和图像上时，它们可能已经毁坏了文件、格式化了硬盘或引发了其他类型的灾害。若是病毒并不寄生于一个污染程序，它仍然能通过占据存储空间给我们带来麻烦，并降低计算机的性能。

出现在计算机领域中的计算机病毒是一组程序，一段可执行码，是一种隐藏在计算机系统的可存取信息资源中，利用系统信息资源进行繁殖并且执行的编码集合。计算机病毒在《中华人民共和国计算机信息系统安全保护条例》第二十八条中明确定义为：“指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据、影响计算机使用，并能够自我复制的一组计算机指令或者程序代码。”

7.1.2　计算机病毒的发展历史

早在 1949 年，计算机先驱者冯·诺依曼就在他的论文《复杂计算机组织论》中，提出了计算机程序能够在内存中自我复制，勾勒出了病毒程序的蓝图。

1983 年 11 月 3 日，弗雷德·科恩博士研制出了一种在运行过程中可以自我复制的破坏性程序，伦·艾德勒曼将它命名为计算机病毒，并在每周一次的安全讨论会上正式提出，8 小时后专家们在 VAX11/750 计算机系统上运行，第一个病毒实验成功，一周后获准推出 5 个实验的演示，从而在实验上验证了计算机病毒的存在。

1985 年初，在巴基斯坦的拉合尔，巴西特和阿姆杰得两兄弟为了防盗版，编写了“巴基斯坦智囊”病毒，该病毒传染软盘引导，一年后病毒以强劲势头流传到了全世界。这是最早在世界上流行的一个真正的病毒。几乎同时，世界各地的计算机用户也发现了形形色色的计算机病毒，如黑色星期五、大麻等。

7.1.3　计算机病毒的特征

在计算机病毒所具有的特征中，传染性、潜伏性、可触发性和破坏性是它的基本特征。



其次，它还有隐蔽性、针对性、衍生性和不可预见性等。

1. 传染性

病毒的传染性也称为自我复制和可传播性，这是计算机病毒的本质特征。在一定条件下，病毒通过某种渠道从一个文件或一台计算机传染到另外没有被感染的文件或计算机，轻则造成被感染的计算机数据或工作失常，重则使计算机瘫痪。病毒代码就是靠这种机制大量传播和扩散的。携带病毒代码的文件称为计算机病毒载体或带毒程序。每一台被感染了病毒的计算机，本身是一个受害者，又是计算机病毒的传播者，通过各种可能的渠道，如软盘、光盘、移动硬盘、网络去传染其他的计算机。在染毒的计算机上曾经使用过的移动硬盘，很有可能已被计算机病毒感染，如果拿到其他机器上使用，病毒就会通过带毒移动硬盘传染这些机器。如果计算机已经联网，通过数据或程序共享，病毒就可以迅速传染与之相连的计算机，若不加以控制，就会在很短的时间内传遍整个世界。

2. 潜伏性

一个编制巧妙的病毒程序，进入系统之后一般不会马上发作，可以在一段时间内隐藏在合法文件中，对其他文件或计算机进行传染，而不被人发现。在此期间，系统的备份设备复制病毒程序，制成程序或数据的副本并送到其他的部位使之感染。它可长期隐藏在系统中，只有在满足其特定条件时才启动其表现（破坏）模块。只有这样，它才能进行广泛的传播。如著名的“黑色星期五”病毒在每逢 13 号的星期五发作。国内的“上海一号”病毒会在每年 3、6、9 月的 13 号发作。这些病毒在平时会隐藏得很好，只有在发作日才会露出本来面目。

3. 可触发性

病毒因某个事件或数值的出现，诱使病毒实施感染或进行攻击的特性称为可触发性。为了隐蔽自己，病毒必须潜伏，少做动作。如果完全不动，一直潜伏的话，病毒既不能感染，也不能进行破坏，便失去了杀伤力。病毒既要隐蔽又要维持杀伤力，它必须具有可触发性。病毒的触发机制就是用来控制感染和破坏动作的频率。病毒具有预定的触发条件，这些条件可能是时间、日期、文件类型或某些特定数据等。病毒运行时，触发机制检查预定条件是否满足，如果满足，启动感染或破坏动作，使病毒进行感染或攻击；如果不满足，使病毒继续潜伏。

4. 破坏性

任何病毒只要侵入系统，都会对系统及应用程序产生不同程度的影响。轻者会降低计算机工作效率，占用系统资源，重者可致系统崩溃。由此特性可将病毒分为良性病毒与恶性病毒。良性病毒可能只显示些画面或播出点音乐、无聊的语句，或者根本没有任何破坏动作，但会占用系统资源。这类病毒较多，如女鬼（Joke.Girlghost）、W-BOOT 等病毒。恶性病毒则有明确的目的，破坏数据、删除文件或加密磁盘、格式化磁盘，有的对数据造成不可挽回的破坏。

5. 隐蔽性

病毒一般是具有很高编程技巧、短小精悍的程序，通常附在正常程序中或磁盘较隐蔽



的地方，也有个别的以隐藏文件的形式出现，目的是不让用户发现它的存在。如果不经过代码分析，病毒程序与正常程序是不容易区别开来的。系统被感染病毒后，一般情况下用户是感觉不到它的存在的，只有其发作，出现不正常反应时用户才知道。

6. 针对性

计算机病毒一般都是针对于特定的操作系统，比如说微软的 Windows XP/2000/2003，或者针对特定的应用程序。例如，有针对 IBM/PC 机及其兼容机的，有针对 Apple 公司的 Macintosh，还有针对 UNIX 操作系统的。

7. 衍生性

这种特性为病毒制造者提供了一种创造新病毒的捷径。分析计算机病毒的结构可知，传染的破坏部分反映了设计者的设计思想和设计目的，但是，这可以被其他掌握原理的人以其个人的企图进行任意改动，从而衍生出一种不同于原版本的新的计算机病毒（又称为变种），这就是它的衍生性。这种变种病毒造成的危害可能比原版病毒严重得多。

8. 不可预见性

不同种类病毒的代码千差万别，病毒的制作技术也在不断地提高，病毒比反病毒软件永远是超前的。新的操作系统和应用系统的出现，软件技术的不断发展，也为计算机病毒提供了新的发展空间，对未来病毒的预测更加困难，这就要求人们不断提高对病毒的认识，增强防范意识。

7.1.4 计算机病毒的种类

计算机病毒的分类方法有很多种。按照基本类型划分，可归纳为 6 种类型，包括引导型病毒、可执行文件病毒、宏病毒、混合型病毒、特洛伊木马型病毒和 Web 网页病毒。

1. 引导型病毒

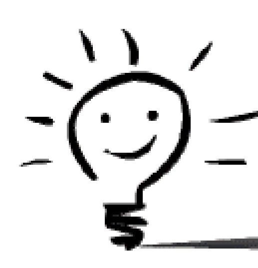
引导型病毒主要是感染软盘、硬盘的引导扇区或主引导扇区，在用户对软盘、硬盘进行读写操作时进行感染活动。我国流行的引导型病毒有 Anti-CMOS、GENP/GENB、Stone、Torch、Monkey 等。

2. 可执行文件病毒

可执行文件病毒主要是感染计算机中的可执行文件（.exe）和命令文件（.com）。文件型病毒是对计算机的源文件进行修改，使其成为新的带毒文件。一旦计算机运行该文件就会被感染，从而达到传播的目的。像我国流行的 Die_Hard、DIR II 等病毒都属此类。

3. 宏病毒

宏病毒是利用高级语言——宏语言编制的病毒。宏病毒仅向 Word、Excel、Access、Power Point 和 Project 等办公自动化程序编制的文档进行传染，而不会传染给可执行文件。由于这些办公处理程序在全球存在着广泛的用户，大家频繁使用这些程序编制文档、电子表格和数据库，并通过移动硬盘、Internet 进行交换，所以，宏病毒的传播十分迅速并非常广泛。



国内流行的宏病毒包括 X2000M.Laroux.A、Concept、Simple2、ethan、7 月杀手等。

4. 混合型病毒

顾名思义，混合型病毒是以上几种病毒的混合。它的破坏性更大，传染的机会也更多，杀灭也更困难。这种病毒扩大了病毒程序的传染途径，它既感染磁盘的引导记录，又感染可执行文件。当染有此种病毒的磁盘用于引导系统或调用执行染毒文件时，病毒都会被激活。因此在检测、清除复合型病毒时，必须全面彻底地根治，如果只发现该病毒的一个特性，把它只当作引导型或文件型病毒进行清除，虽然好像是清除了，但还留有隐患，这种经过消毒后的“洁净”系统更赋有攻击性。这种病毒包括 Flip 病毒、新世纪病毒、One-half 病毒等。

5. 特洛伊木马型病毒

特洛伊木马型病毒也叫黑客程序或后门病毒。一般这种病毒分成服务器端和客户端两部分，如计算机网络中服务器端被此程序感染，别人可通过网络中其他计算机任意控制此计算机，并获得重要文件。国内流行的此类病毒包括 QQ 大盗、鬼影、Trojan.Win32.Fednu.umz 等。

6. Web 网页病毒

随着 Internet 的发展，Web 网页技术逐渐被广泛应用，某些病毒虽然从现在的发展情况来看并不能破坏硬盘上的资料，但是如果用户使用浏览器来浏览含有这些病毒的网页，浏览器就会把这些程序抓下来，然后用使用者自己系统里的资源去执行，因而，使用者就在不知不觉的状态下，被病毒进入机器进行复制并通过网络窃取宝贵的个人信息，或使计算机系统资源利用率下降，造成死机现象，并且该病毒会在一台一台的终端上不断传播。这类病毒包括欢乐时光（VBS.Happytime）、十四日（Js.Fortnight.c.s）等。

7.1.5 计算机病毒的工作原理

认清计算机病毒的结构和主要特征，了解计算机病毒工作的一般过程及原理，可以为我们检测和清除病毒提供充实可靠的依据，针对每个环节做出相应的防范措施。

1. 计算机病毒的工作过程

计算机病毒的完整工作过程一般应包括以下几个环节。

（1）传染源：病毒总是依附于某些存储介质，如软盘、硬盘等构成传染源。

（2）传染媒介：病毒传染的媒介由工作环境来决定，可能是计算机网络，也可能是可移动的存储介质，如移动硬盘等。

（3）病毒激活：是指将病毒装入内存，并设置触发条件，触发的条件是多样化的，可以是内部时钟、系统的日期、用户标识符，也可能是系统一次通信等。一旦触发条件成熟，病毒就开始作用，自我复制到传染对象中，进行各种破坏活动等。

（4）病毒表现：表现是病毒的主要目的之一，有时在屏幕上显示出来，有时则表现为破坏系统数据。可以这样说，凡是软件技术能够触发到的地方，都在其表现范围内。

（5）传染：病毒的传染是病毒性能的一个重要标志。在传染环节中，病毒复制一个自身副本到传染对象中去。

2. 计算机病毒的引导机制

（1）计算机病毒的寄生对象。

计算机病毒存储在磁盘上，为了进行自身的主动传播，必须寄生在可以获得执行权的寄生对象上。就目前出现的各种计算机病毒来看，其寄生对象有两种，一种是寄生在磁盘引导扇区；另一种是寄生在可执行文件（.exe 或.com）中。不论是磁盘引导扇区还是可执行文件，它们都有获取执行权的可能，病毒程序寄生在它们上面，就可以在一定条件下获得执行权，从而使病毒得以进入计算机系统，并处于激活状态，然后进行病毒的动态传播和破坏活动。

（2）计算机病毒的寄生方式。

计算机病毒的寄生方式有两种，一种是采用替代法；另一种是采用链接法。所谓替代法是指病毒程序用自己的部分或全部指令代码，替代磁盘引导扇区或文件中的全部或部分内容；所谓链接法则是指病毒程序将自身代码作为正常程序的一部分与原有正常程序链接在一起，病毒链接的位置可能在正常程序的首部、尾部或中间。寄生在磁盘引导扇区的病毒一般采取替代法，而寄生在可执行文件中的病毒一般采用链接法。

（3）驻留内存。

计算机病毒若要发挥破坏作用，要开辟所用内存空间或覆盖系统占用的部分内存空间以便驻留内存。当病毒程序驻留内存后，必须使有关部分取代或扩充系统的原有功能，并窃取系统的控制权。此后病毒程序依据其设计思想，隐藏自己，等待时机，在条件成熟时，再进行传染和破坏。

病毒为隐藏自己，驻留内存后还要恢复系统，使系统不会死机，只有这样才能等待时机成熟后，进行感染和破坏。有的病毒在加载之前进行动态反跟踪和病毒体解密。

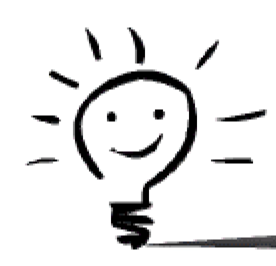
对于寄生在磁盘引导扇区的病毒来说，病毒引导程序占用了原系统引导程序的位置，并把原系统引导程序转移到一个特定的地方。这样系统一启动，病毒引导模块就会自动地装入内存并获得执行权，然后该引导程序负责将病毒程序的传染模块和发作模块装入内存的适当位置，并采取常驻内存技术以保证这两个模块不会被覆盖，接着对这两个模块设定某种激活方式，使之在适当的时候获得执行权。这些工作完成后，病毒引导模块装入内存，使系统在带病毒的状态下运行。

对于寄生在可执行文件中的病毒来说，病毒程序一般通过修改原有可执行文件，使该文件执行时首先转入病毒程序引导模块，该引导模块负责把病毒程序的其他两个模块驻留内存及进行初始化的工作，然后把执行权交给执行文件，使系统及执行文件在带毒的状态下运行。

3. 计算机病毒的触发机制

传染、潜伏、可触发、破坏是病毒的基本特性。可触发性是病毒的攻击性和潜伏性之间的调整杠杆，可以控制病毒感染和破坏的频度，兼顾杀伤力和潜伏性。

过于苛刻的触发条件，可能使病毒有好的潜伏性，但不易传播，杀伤力较低。而过于



宽松的触发条件将导致病毒频繁感染与破坏，容易暴露，导致用户做出反病毒处理，也不能有大的杀伤力。

计算机病毒在传染和发作之前，往往要判断某些特定条件是否满足，满足则传染或发作，否则不传染、不发作或只传染不发作，这个条件就是计算机病毒的触发条件。

实际上病毒采用的触发条件花样繁多，目前病毒采用的触发条件主要有以下几种。

（1）时间触发：它包括特定的时间触发、染毒后累计工作时间触发、文件最后写入时间触发等。

（2）键盘触发：有些病毒监视用户的击键动作，当发现病毒预定的输入时，病毒被激活，进行某些特定操作。键盘触发包括击键次数触发、组合键触发、热启动触发等。

（3）日期触发：许多病毒采用日期作触发条件。日期触发大体包括特定日期触发、月份触发、前半年或后半年触发等。

（4）启动触发：病毒对机器的启动次数计数，并将此值作为触发条件。

（5）访问磁盘次数触发：病毒对磁盘 I/O 访问的次数进行计数，以预定次数做为触发条件。

（6）调用中断功能触发：病毒对中断调用次数计数，以预定次数做为触发条件。

被计算机病毒使用的触发条件是多种多样的，而且往往不只是使用上面所述的某一个条件，而是使用多个条件组合起来的触发条件。大多数病毒的组合触发条件是基于时间的，再加上读、写操作，按键操作以及其他条件。如“侵略者”病毒的激发时间是开机后机器运行时间和病毒传染个数成某个比例时，恰好按 Ctrl+Alt+Delete 组合键试图重新启动系统则病毒发作。

病毒中有关触发机制的编码是其敏感部分。剖析病毒时，如果搞清病毒的触发机制，可以修改此部分代码，使病毒失效，从而产生没有潜伏性的极为外露的病毒样本，供反病毒研究使用。

4. 计算机病毒的破坏行为

计算机病毒的破坏行为体现了病毒的杀伤能力。病毒破坏行为的激烈程度取决于病毒作者的主观愿望和他所具有的技术能量。数以万计、不断发展扩张的病毒，其破坏行为千奇百怪，不可能穷举其破坏行为。我们可以把病毒的破坏目标和攻击部位归纳如下。

（1）攻击系统数据区。攻击部位包括硬盘主引导区、Boot 扇区、FAT 表、文件目录。一般说来，攻击系统数据区的病毒是恶性病毒，受损的数据不易恢复。

（2）攻击文件。病毒对文件的攻击方式有很多，包括删除、改名、替换内容、丢失部分程序代码、内容颠倒、写入时间空白、变碎片、假冒文件、丢失文件簇和丢失数据文件。

（3）攻击内存。内存是计算机的重要资源，也是病毒的攻击目标。病毒额外地占用和消耗系统的内存资源，可以导致一些大程序受阻。病毒攻击内存的方式包括占用大量内存、改变内存总量、禁止发配内存和蚕食内存。

（4）干扰系统运行。病毒会干扰系统的正常运行，以此作为自己的破坏行为。此类行为也是花样繁多，例如，不执行命令、干扰内部命令的执行、虚假报警、打不开文件、内部栈溢出、占用特殊数据区、换现行盘、时钟倒转、重启动、死机、强制游戏、扰乱串并口。

（5）运行速度下降。病毒激活时，其内部的时间延迟程序启动。在时钟中纳入了时间的循环计数，迫使计算机空转，计算机速度明显下降。

（6）攻击磁盘。其包括攻击磁盘数据、不写盘、写操作变读操作、写盘时丢字节。

（7）攻击 CMOS。在机器的 CMOS 区中，保存着系统的重要数据，例如系统时钟、磁盘类型、内存容量等，并具有校验和。有的病毒激活时，能够对 CMOS 区进行写入动作，破坏系统 CMOS 区中的数据。

5. 计算机病毒的传播

（1）计算机病毒传播的一般过程。

在系统运行时，计算机病毒通过病毒载体即系统的外存储器进入系统的内存储器，常驻内存。该病毒在系统内存中监视系统的运行，当它发现有攻击的目标存在并满足条件时，便从内存中将自身存入被攻击的目标，从而将病毒进行传播。而病毒利用系统 INT 13H 写磁盘的中断又将其写入系统的外存储器软盘或硬盘中，再感染其他系统。

（2）计算机病毒的传播途径。

计算机病毒具有自我复制和传播的特点，因此，研究计算机病毒的传播途径是极为重要的。从计算机病毒的传播机制分析可知，只要是能够进行数据交换的介质都可能成为计算机病毒传播途径。现在通过 Internet 传播计算机病毒与过去手工传播计算机病毒的方式相比速度要快得多。

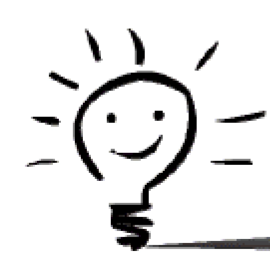
目前，网络和电子邮件已经成为最重要的病毒传播途径。此外，传统的软盘、光盘等传播方式也占据了一定的比例。

网络是由相互连接的一组计算机组成的，这是数据共享和相互协作的需要。数据能从一台计算机发送到其他计算机上。如果发送的数据感染了计算机病毒，接收方的计算机将自动被感染，因此有可能在很短的时间内感染整个网络中的计算机。

局域网技术的应用为企业的发展作出了巨大贡献，同时也为计算机病毒的迅速传播创造了条件。特别是国际互联网，已经越来越多地被用于获取信息、发送和接收文件、接收和发布新的消息以及下载文件的程序。随着互联网的高速发展，计算机病毒也走上了高速传播之路，已经成为计算机病毒的第一传播途径。除了传统的文件型计算机病毒以文件下载、电子邮件的附件等形式传播外，新兴的电子邮件计算机病毒，如“美丽莎”计算机病毒、“我爱你”计算机病毒等则是完全依靠网络来传播。甚至还有利用网络分布计算机技术将自身分成若干部分，隐藏在不同的主机上进行传播的计算机病毒。

目前，移动硬盘是使用广泛、移动频繁的存储介质，因此也成了计算机病毒寄生的“温床”。盗版光盘上的软件和游戏及非法复制也是目前传播计算机病毒的主要途径。硬盘是数据的主要存储介质，因此也是计算机病毒感染的重灾区。硬盘传播计算机病毒的途径体现在：硬盘在移动硬盘上复制带毒文件、带毒情况下格式化另一硬盘、向光盘上刻录带毒文件和硬盘之间的数据复制，以及将带毒文件发送到其他地方等。

计算机病毒也可以通过点对点通信系统和无线通道传播。但目前这种传播途径还不是十分广泛，但预计在未来的信息时代，这种途径很可能与网络传播途径成为病毒扩散的两大途径。



7.1.6 计算机病毒的检测、防范和清除

随着网络的发展，伴随而来的计算机病毒传播问题越来越引起人们的关注。互联网的普及使有些计算机病毒借助网络爆发流行，如 2012 年主要流行的 U 盘寄生虫及其变种、网游窃贼及其变种、代理木马及其变种等病毒，它们与以往的计算机病毒相比具有一些新的特点，给广大计算机用户带来了极大的损失。

在与计算机病毒的对抗中，如果能采取有效的防范措施，就能使系统不染毒，或者染毒后减少损失。当计算机系统或文件染有计算机病毒时，需要检测和清除。但是，隐性计算机病毒和多态性计算机病毒使人难以检测。

1. 计算机病毒的检测

判断自己的计算机中是否染有病毒，最简单的方法是用较新的防病毒软件对磁盘进行全面的检测。无论什么病毒，在其入侵系统后总会留下一些“蛛丝马迹”。如何及早地发现新病毒呢？

用户可以用下面简单的方法判断：首先应注意内存情况，绝大部分的病毒是要驻留内存的，应注意被占用的内存数是否无故减少。其次应注意常用的可执行文件（如 command.com）的字节数，绝大多数的病毒在对文件进行传染后会使文件的长度增加。在查看文件字节数时应首先用干净系统盘启动。

如出现软件运行速度变慢（磁盘读盘速度影响除外）、输出端口异常等现象都有可能是病毒造成的。最准确的方法是查看中断向量及引导扇区是否被无故改变，这就需要对系统及磁盘格式有一定的了解。

常用的检测病毒方法包括特征代码法、校验和法、行为监测法、软件模拟法，这些方法依据的原理不同，实现时所需的开销不同，检测的范围也不同，其各有所长。

（1）特征代码法。

特征代码法早期被应用于 SCAN、CPAV 等著名病毒检测工具中。国外专家认为特征代码法是检测已知病毒的最简单、开销最小的方法。

特征代码法的实现步骤如下：采集已知病毒样本，病毒如果既感染.com 文件又感染.exe 文件，对这种病毒要同时采集.com 型病毒样本和.exe 型病毒样本。在病毒样本中，抽取特征代码。

依据如下原则：抽取的代码比较特殊，不大可能与普通正常程序代码吻合。抽取的代码要有适当长度，一方面维持特征代码的唯一性，另一方面又不要有太大的空间与时间的开销。如果一种病毒的特征代码增长 1 字节，要检测 3000 种病毒，增加的空间就是 3000 字节。在保持唯一性的前提下，尽量使特征代码长度短些，以减少空间与时间的开销。在既感染.com 文件又感染.exe 文件的病毒样本中，要抽取两种样本共有的代码，将特征代码纳入病毒数据库中。

打开被检测文件，在文件中搜索，检查文件中是否含有病毒数据库中的病毒特征代码。如果发现病毒特征代码，由于特征代码与病毒一一对应，便可以断定，被查文件中含有何种病毒。

采用病毒特征代码法的检测工具，面对不断出现的新病毒，必须不断更新版本，否则检测工具便会老化，逐渐失去实用价值。病毒特征代码法对从未见过的新病毒，自然无法知道其特征代码，因而无法去检测这些新病毒。

特征代码法检测准确快速，可识别病毒的名称，误报警率低，依据检测结果，可做解毒处理。但不能检测未知病毒、需搜集已知病毒的特征代码、费用开销大、在网络上效率低（在网络服务器上，因长时间检索会使整个网络性能降低）是它的缺点。

（2）校验和法。

计算正常文件内容的校验和，将该校验和写入文件中或写入别的文件中保存。在文件使用过程中，定期地或每次使用文件前，检查文件现在内容算出的校验和与原来保存的校验和是否一致，因而可以发现文件是否感染，这种方法叫校验和法，它既可发现已知病毒又可发现未知病毒。在 SCAN 和 CPAV 工具的后期版本中除了病毒特征代码法之外，还纳入校验法，以提高其检测能力。

这种方法不能识别病毒类，不能报出病毒名称。由于病毒感染并非文件内容改变的唯一的非他性原因，文件内容的改变有可能是正常程序引起的，所以校验和法常常误报警。而且此种方法也会影响文件的运行速度。

病毒感染的确会引起文件内容变化，但是校验和法对文件内容的变化太敏感，又不能区分正常程序引起的变动，从而频繁报警。用监视文件的校验和来检测病毒，不是最好的方法。

这种方法遇到下述情况：已有软件版本更新、变更口令、修改运行参数，校验和法都会误报警。

校验和法对隐蔽性病毒无效。隐蔽性病毒进驻内存后，会自动剥去染毒程序中的病毒代码，使校验和法受骗，对一个有毒文件算出正常校验和。

校验和法简单、能发现未知病毒、被查文件的细微变化也能发现。但发布通行记录正常态的校验和、会误报警、不能识别病毒名称、不能对付隐蔽型病毒是它的缺点。

（3）行为监测法。

行为监测法是指利用病毒的特有行为特征来监测病毒的方法。病毒有一些共同行为，而且比较特殊。在正常程序中，这些行为比较罕见。当程序运行时，监视其行为，如果发现了病毒行为，立即报警。

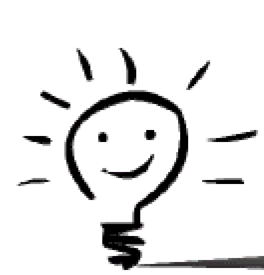
作为监测病毒的行为特征可列举如下：

① 占有 INT 13H 所有的引导型病毒，都攻击 Boot 扇区或主引导扇区。系统启动时，当 Boot 扇区或主引导扇区获得执行权时，系统刚刚工作。一般引导型病毒都会占用 INT 13H 功能，因为其他系统功能未设置好，无法利用。引导型病毒占据 INT 13H 功能，在其中放置病毒所需的代码。

② 修改 DOS 系统为数据区的内存总量。病毒常驻内存后，为了防止 DOS 系统将其覆盖，必须修改系统内存总量。

③ 运行.com 或.exe 文件。病毒要感染的条件是必须运行.com 或.exe 文件。

④ 病毒程序与原主程序的切换。染毒程序运行中，先运行病毒，然后运行原主程序。在两者切换时，有许多特征行为。



行为监测法可以发现未知病毒、可相当准确地预报未知的多数病毒。可能误报警、不能识别病毒名称、实现时有一定难度是它的缺点。

（4）软件模拟法。

用来检测多态病毒。为了检测多态病毒，反病毒专家研制了一种新的检测方法——软件模拟法。它是一种软件分析器，在机器的虚拟内存中用软件方法来模拟和分析不明程序的运行，而且程序的运行不会对系统各部分起实际的作用，因而不会对系统造成危害。在执行过程中，从虚拟机环境内截获文件数据，如果含有可疑病毒代码，则杀毒后将其还原到原文件中，从而实现检测多态病毒。

2. 计算机病毒的防范

防范是对付计算机病毒的积极而又有效的措施，比等待计算机病毒出现之后再去扫描和清除能更有效地保护计算机系统。要做好计算机病毒的防范工作，首先是防范体系和制度的建立；其次利用反病毒软件及时发现计算机病毒侵入，对它进行监视、跟踪等操作，并采取有效的手段阻止它的传播和破坏。

老一代的反病毒软件只能对计算机系统提供有限的保护，只能识别出已知的计算机病毒。新一代的反病毒软件则不仅能识别出已知的计算机病毒，在计算机病毒运行前就发出警报，还能屏蔽掉计算机病毒程序的传染和破坏功能，使受感染的程序可以继续运行（即所谓的带毒运行）。同时还能利用计算机病毒的行为特征，防范未知计算机病毒的侵扰和破坏。另外，新一代的反病毒软件还能实现超前防御，将系统中可能被计算机病毒利用的资源都加以保护，不给计算机病毒可乘之机。

计算机病毒的工作方式是可以分类，反病毒软件就是针对已归纳总结出的这几类计算机病毒工作方式来进行防范的。当被分析过的已知计算机病毒出现时，由于其工作方式早已被记录在案，反病毒软件能识别出来；当未曾被分析过的计算机病毒出现时，如果其工作方式仍可被归入已知的工作方式，则这种计算机病毒能被反病毒软件所捕获。这也是采取积极防御措施的计算机病毒防范方法优越于传统方法的地方。

当然，如果新出现的计算机病毒不按已知的方式工作，这种新的传染方式又不能被反病毒软件所识别，那么反病毒软件也无能为力了。

这时只能采取两种措施进行保护：第一是依靠管理上的措施，及早发现疫情，捕捉计算机病毒，修复系统。第二是选用功能更加完善的、具有更强超前防御能力的反病毒软件，尽可能多地堵住能被计算机病毒利用的系统漏洞。

对于病毒，人们虽然使用了许多种反病毒软件，但仍经常受到病毒的攻击。维护计算机的安全是一项漫长的过程。

反病毒软件常用以下几种反病毒技术来对病毒进行预防和彻底杀除。

（1）实时监视技术。

这个技术为计算机构筑起一道动态、实时的反病毒防线，通过修改操作系统，使操作系统本身具备反病毒功能。时刻监视系统当中的病毒活动、系统状况，时刻监视软盘、光盘、互联网、电子邮件上的病毒传染，将病毒阻止在操作系统外部。优秀的反病毒软件由于采用了与操作系统的底层无缝连接技术，实时监视器占用的系统资源极小，用户一方面



完全感觉不到对机器性能的影响，一方面根本不用考虑病毒的问题。

只要反病毒软件实时地在系统中工作，病毒就无法入侵我们的计算机系统。可以保证反病毒软件只需一次安装，今后计算机运行的每一秒钟都会执行严格的反病毒检查，使互联网、光盘、软盘等途径进入计算机的每一个文件都安全无毒，如有毒则自动杀除。

（2）全平台反病毒技术。

目前病毒活跃的平台包括 Windows XP/ 2000/2003、UNIX 等，为了反病毒软件做到与系统的底层无缝连接，可靠地实时检查和杀除病毒，必须在不同的平台上使用相应平台的反病毒软件，如用的是 Windows 的平台，则必须用 Windows 版本的反毒软件。如果是企业网络，什么版本的平台都有，那么就要在网络的每一个 Server、Client 端上安装 Windows XP/2000/2003、UNIX 等平台的反病毒软件，每一个点上都安装相应的反病毒模块，每一个点上都能实时地抵御病毒攻击。只有这样，才能作到网络的真正安全和可靠。

7.2　网络病毒的防范和清除

按照计算机病毒的传播媒介来分类，可分为单机病毒和网络病毒。

单机病毒就是以前的 DOS 病毒、Windows 病毒和能在多操作系统下运行的宏病毒。单机病毒的载体是磁盘，常见的是病毒从软盘传入硬盘，感染系统，然后再传染其他软盘，软盘又传染其他系统。

网络病毒通过计算机网络传播感染网络中的可执行文件，它的传播媒介不再是移动式载体，而是网络通道，这种病毒的传染能力更强，破坏力更大。

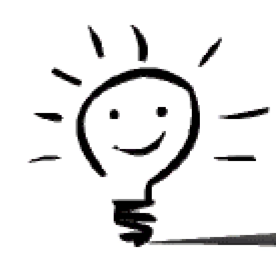
1. 网络病毒的防范措施

相对于单机病毒的防护来说网络病毒的防范具有更大的难度，网络病毒的防范应与网络管理集成。网络防病毒的最大优势在于网络的管理功能，如果没有把管理功能加上，很难完成网络防毒的任务，只有管理与防范相结合，才能保证系统的良好运行。管理功能就是管理全部的网络设备与操作，从 Hub、交换机、服务器到 PC，包括软盘的存取、局域网上的信息互通与 Internet 的接驳等所有病毒能够感染和传播的途径。

在网络环境下，病毒传播扩散快，仅用单机反病毒产品已经难以清除网络病毒，必须有适用于局域网、广域网的全方位反病毒产品。

在选用反病毒软件时，应选择对病毒具有实时监控能力的软件，这类软件可以在第一时间阻止病毒感染，而不是靠事后去杀毒。要养成定期升级防病毒软件的习惯，并且间隔时间不要太长，因为绝大部分反病毒软件的查毒技术都是基于病毒特征码的，即通过对已知病毒提取其特征码，并以此来查杀同种病毒。对于每天都可能出现的新病毒，反病毒软件会不断更新其特征码数据库。

要养成定期扫描文件系统的习惯；对移动硬盘、光盘等移动存储介质，在使用之前应进行查毒；对于从网上下载的文件和电子邮件附件中的文件，在打开之前也要先杀毒。另外，由于防病毒软件总是滞后于病毒，因此它通常不能发现一些新的病毒。因此，不能只



依靠防病毒软件来保护系统。在使用计算机时，还应当注意以下几点。

（1）不使用或下载来源不明的软件。

（2）不轻易上一些不正规的网站。

（3）提防电子邮件病毒的传播。一些邮件病毒会利用 ActiveX 控件技术，当以 HTML 方式打开邮件时，病毒可能就会被激活。

（4）经常关注一些网站、论坛发布的病毒报告，这样可以在未感染病毒时做到预先防范。

（5）及时更新操作系统，为系统漏洞打上补丁。

（6）重要数据、文件要定期备份。

2. 网络病毒的清杀

一旦在网络上发现病毒，应设法立即清除，其操作步骤如下。

（1）立即通知所有用户下网，关闭文件服务器。

（2）用带有写保护的、干净的系统盘启动系统管理员工作站，并立即清除本机病毒。

（3）用带有写保护的、干净的系统盘启动文件服务器。系统管理员登录并下命令禁止其他用户登录。

（4）将文件服务器硬盘中的重要资料备份。但严禁执行硬盘上的程序和在硬盘中复制文件，以免破坏被病毒搞乱的硬盘数据结构。

（5）用杀毒软件扫描服务器上所有的文件，恢复或删除被病毒感染的文件，重新安装被删除的文件。

（6）用杀毒软件扫描并清除所有可能染上病毒的移动盘或备份文件中的病毒。

（7）用杀毒软件扫描并清除所有的有盘工作站硬盘上的病毒。

（8）在确信病毒已经彻底清除后，重新启动网络和工作站。

7.3 典型网络病毒的介绍

7.3.1 宏病毒

1. 宏病毒的定义

宏病毒是一种寄存在文档或模板的宏中的计算机病毒。一旦打开这样的文档，其中的宏就会被执行，于是宏病毒就会被激活，转移到计算机上，并驻留在 Normal 模板上。从此以后，所有自动保存的文档都会“感染”上这种宏病毒，而且如果其他用户打开了感染病毒的文档，宏病毒又会转移到他的计算机上。

所谓宏，就是一些命令组织在一起，作为一个单独命令完成一个特定任务。Microsoft Word 中将宏定义为：“宏就是能组织到一起作为一独立的命令使用的一系列 Word 命令，它能使日常工作变得更容易。”Word 使用宏语言 WordBasic 将宏作为一系列指令来编写。

宏病毒是针对微软公司的 Office 办公软件编写的一种病毒。微软公司的 Office 办公软



件是最为流行的编辑软件，并且跨越了多种系统平台，宏病毒充分利用了这一点得到广泛传播。宏病毒作为一种新型病毒有其特点与共性。

2. 宏病毒的特征

宏病毒具有以下特征。

（1）传播极快。

Word 宏病毒通过.doc 文档及.dot 模板进行自我复制及传播，而计算机文档是交流最广的文件类型。人们大多重视保护自己计算机的引导部分和可执行文件不被病毒感染 ，而对外来的文档文件基本是直接浏览使用，这给 Word 宏病毒传播带来很多便利。特别是 Internet 的普及，E-mail 的大量应用更为 Word 宏病毒传播铺平道路。根据国外较保守的统计，宏病毒的感染率高达 40%以上，即在现实生活中每发现 100 个病毒，其中就有 40 多个宏病毒，而国际上普通病毒种类已达 12000 多种。

（2）制作、变种方便。

以往病毒是以二进制的计算机机器码形式出现，而宏病毒则是以人们容易阅读的源代码宏语言 WordBasic 形式出现，所以编写和修改宏病毒比以往更容易。世界上的宏病毒原型已有几十种，其变种与日俱增，追究其原因还是 Word 的开放性所致。现在的 Word 病毒都是用 WordBasic 语言所写成，大部分 Word 宏病毒并没有使用 Word 提供的 Execute-Only 处理函数处理，它们仍处于可打开阅读、修改状态。所有用户在 Word 工具的宏菜单中很方便就可以看到这种宏病毒的全部面目。当然会有“不法之徒”利用掌握的 Basic 语句简单知识把其中的病毒激活条件和破坏条件加以改变，立即就生产出了一种新的宏病毒，甚至比原病毒的危害更加严重。

（3）破坏可能性极大。

鉴于宏病毒用 WordBasic 语言编写，WordBasic 语言提供了许多系统级底层调用，如直接使用 DOS 系统命令、调用 WindowsAPI、调用 DDE 或 DLL 等。这些操作均可能对系统直接构成威胁，而 Word 在指令安全性、完整性上检测能力很弱，破坏系统的指令很容易被执行。宏病毒 Nuclear 就是破坏操作系统的典型一例。

（4）多平台交叉感染。

宏病毒冲破了以往病毒在单一平台上传播的局限，当 Word、Excel 这类著名应用软件在不同平台（如 Windows、Windows NT、OS/2 和 Macintosh 等）上运行时，会被宏病毒交叉感染。

3. 宏病毒的防范和清除

宏病毒的防治和清除方法如下。

（1）使用“提示保存 Normal 模板”选项。

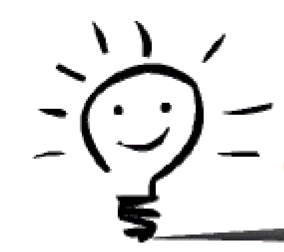
（2）不要通过 Shift 键来禁止运行自动宏。

（3）查看宏代码并删除。

（4）使用 Disable Auto Macros 宏。

（5）设置 Normal.dot 的只读属性。

（6）Normal.dot 的密码保护。



7.3.2 电子邮件病毒

风靡全球的“美丽莎”（Melissa）、Papa 和 HAPPY99 等计算机病毒正是通过电子邮件的方式进行传播、扩散的，其结果是导致邮件服务器瘫痪、用户信息和重要文档泄密、无法收发 E-mail，给个人、企业和政府部门造成了严重的损失。为此有必要介绍一下电子邮件计算机病毒。

电子邮件计算机病毒实际上并不是一类单独的计算机病毒，严格地说它应该划入到文件型计算机病毒及宏病毒中去，只不过由于这些病毒采用了独特的电子邮件传输方式（其中不少种类还专门针对电子邮件的传播方式进行了优化），因此我们习惯于将它们称为电子邮件病毒。

所谓电子邮件病毒就是以电子邮件作为传播途径的计算机病毒，实际上该类病毒和普通的病毒一样，只不过是传播方式改变而已。该类计算机病毒的特点包括以下几方面。

（1）电子邮件本身是无毒的，但它的内容中可以有 UNIX 下的特殊的换码序列，就是通常所说的 ANSI 字符，当用 UNIX 智能终端上网查看电子邮件时，有被侵入的可能。

（2）电子邮件可以夹带任何类型的文件作为附件（Attachment），附件文件可能带有病毒。

（3）可利用某些电子邮件收发器特有的扩充功能，比如 Outlook/Outlook Express 能够执行 VBA 指令编写的宏，在电子邮件中夹带有针对性的代码，利用电子邮件进行传染、扩散。

（4）超大的电子邮件或电子邮件炸弹也可以被认为是一种电子邮件计算机病毒，它能够影响邮件服务器的正常服务功能。

通常对付电子邮件计算机病毒，只要删除携带电子邮件计算机病毒的信件就能够删除它。但是大多数的电子邮件计算机病毒一被接收到客户端时就开始发作了，基本上没有潜伏期。所以预防电子邮件计算机病毒是至关重要的。以下是一些常用的预防电子邮件计算机病毒的方法。

（1）及时下载安装操作系统的漏洞补丁程序，同时也要关注热门第三方应用软件的漏洞更新。

（2）及时升级计算机系统中防病毒软件和防火墙。

（3）不要随意单击或运行通过 QQ、MSN、电子邮件发来的陌生链接地址或文件。

（4）提高自己私密性数据的安全，最好经常更换或是设置比较复杂的账户密码。

对付电子邮件计算机病毒，还可以在计算机上安装有电子邮件实时监控功能的防杀计算机病毒软件。有条件的还可以在电子邮件服务器上安装服务器版电子邮件计算机病毒防护软件，从外部切断电子邮件计算机病毒的入侵途径，确保整个网络的安全。

7.3.3 网络病毒实例

1. 电子邮件炸弹

电子邮件炸弹是指发件者以不明来历的电子邮件地址，不断重复地将电子邮件发送给



同一个人。由于其情况就像是战争时利用某种战争工具对同一个地方进行大轰炸，因此称为电子邮件炸弹。

电子邮件炸弹之所以可怕，是因为它可以大量消耗网络资源。一般网络用户 E-mail 信箱的容量都是有限的，如果你在短时间内收到上千个电子邮件，而每个电子邮件又占据了一定的容量，一个电子邮件炸弹的总容量很容易就超过用户的 E-mail 信箱所能够承受的负荷。在这样的情况下，用户的电子邮箱不仅不能再接收其他人发送来的电子邮件，也随时会因为“超载”而导致整个计算机瘫痪。

没有人知道自己什么时候会碰到电子邮件炸弹，所以采取防范措施是必要的，比较有效的防御方式是，用户可以在电子邮件中安装一个过滤器，在接收任何电子邮件之前预先检查发件人的资料，如果觉得有可疑之处，可以将它删除，不让它进入你的电子邮箱。

2. 恶意网页

（1）恶意网页的原理。

对于恶意网页，常常采取 VBScript 和 JavaScript 编程的形式，由于编程方式十分简单，所以在网上非常流行。VBScript 和 JavaScript 是由微软操作系统的 WSH（Windows Scripting Host，Windows 脚本主机）解析并执行的，由于其编程非常简单，所以此类脚本病毒在网上疯狂传播，疯狂一时的“爱虫”病毒就是一种 VBScript 脚本病毒，然后伪装成邮件附件诱惑用户单击运行，更为可怕的是，这样的病毒是以源代码的形式出现的，只要懂得一点关于脚本编程的人就可以修改其代码，形成各种各样的变种。例如：

```
Set objFs=CreateObject
("Scripting.FileSystem Object")              //创建一个文件系统对象
objFs.CreateTextFile("C:\simple.txt",1)       //通过文件系统对象的方法创建了 TXT 文件
```

如果我们把这句话保存为.vbs 的 VB 脚本文件，单击它就会在 C 盘中创建一个 TXT 文件了。

倘若我们把第二句改为：objFs.GetFile(Wscript.ScriptFullName)Copy(“C:\simple.vbs”)，就可以将自身复制到 C 盘 simple.vbs 这个文件中。本句前面是打开这个脚本文件，Wscript.ScriptFullName 指明是这个程序本身，是一个完整的路径文件名。GetFile 函数获得这个文件，Copy 函数将这个文件复制到 C 盘根目录下 simple.vbs 这个文件中。这么简单的两句代码就实现了自我复制的功能，它已经具备病毒的基本特征——自我复制能力。

此类病毒往往是通过邮件传播的。在 VBScript 中调用邮件发送功能也非常简单，病毒往往采用的方法是向 Outlook 的地址簿中的邮件地址发送带有包含自身的邮件来达到传播的目的，此类病毒的变种繁多，破坏力极大，同时也是非常难以根除的。

（2）恶意网页的预防。

① 禁用 WSH（Windows Scripting Host）。WSH 运行各种类型的文本，但基本都是 VBScript 或 JavaScript。WSH 在文本语言之间充当翻译的角色，该语言可能支持 ActiveXScripting 界面，WSH 运行各种类型的文本，但基本都是 VBScript 或 JavaScript。WSH 在文本语言之间充当翻译的角色，该语言支持 ActiveXScripting 界面，包括 VBScript、



JavaScript、Perl 及所有 Windows 操作的功能，如访问文件夹、文件快捷方式、网络接入和 Windows 注册等。许多病毒或蠕虫就是使用 WSH 入侵到主机。禁用 WSH 的方法是：在 IE 窗口中选择“工具”→“Internet 选项”命令，在弹出的对话框中选择“安全”选项卡，再单击“自定义级别”按钮，就会弹出“安全设置”对话框，把其中所有 ActiveX 插件和控件以及与 Java 相关的全部选项设为“禁用”。但是，这样做在以后的网页浏览过程中有可能会使一些正常应用 ActiveX 的网站无法浏览。

② 不要轻易去访问陌生的站点，有可能里面就含有恶意代码。因为这一类网页主要是含有恶意代码的 ActiveX 或 Applet、JavaScript 的网页文件，所以在 IE 设置中将 ActiveX 插件和控件、Java 脚本等全部禁止就可以大大减少被网页恶意代码感染的机率。其方法是：当运行 IE 时，选择“工具”→“Internet 选项”→“安全”→“Internet 区域的安全级别”选项，把安全级别由“中”改为“高”。

③ 不随意查看陌生邮件，尤其是带有附件的邮件。因为 Windows 允许文件名使用多个后缀，而电子邮件一般只显示第一个后缀，如.jpg，而该文件可能是.jpg.vbs，打开这个文件可能意味着运行一个恶意的 VBScript 病毒，而不是.jpg 查看器。病毒邮件能够利用 IE 和 Outlook 的漏洞自动执行，所以计算机用户需要升级 IE 和 Outlook 程序及常用的其他应用程序。

④ 安装防病毒产品并保证更新最新的病毒特征码。首次安装病毒软件时，一定要对机器做一次彻底扫描，以确保它未受到过病毒的感染，并且用户应当及时更新病毒库。

7.4 常用杀毒软件的介绍

随着世界范围内计算机病毒的大量流行，新的病毒不断出现，各种反病毒软件产品也在不断地推陈出新、更新换代。这些产品的特点表现为技术领先、误报率低、杀毒效果明显、界面友好、良好的升级和售后服务技术支持、与各种软硬件平台兼容性好等方面。常用的国产反病毒软件有瑞星杀毒软件 2012、金山杀毒软件、江民杀毒软件 KV2012 等。

7.4.1 瑞星杀毒软件

瑞星杀毒软件 2012，是北京瑞星科技股份有限公司采用最新技术开发的新一代信息安全产品。以变频杀毒引擎为核心，通过变频技术使计算机得到安全保证的同时，又大大降低资源占用，让计算机更加轻便。同时，瑞星 2012 版应用“瑞星云安全+”技术、“云查杀”、“网购保护”、“智能、安全上网”和智能反钓鱼等技术，保护网购、网游、微博、办公等常见应用面临的各种安全问题，通过友善易用的界面和更小的资源占用为用户提供全新安全软件体验。

瑞星杀毒软件 2012 具体的功能如下。

（1）瑞星变频杀毒技术：智能检测计算机资源占用，自动分配杀毒时占用的系统资源，既保障计算机正常使用，又保证计算机安全。



（2）瑞星“云查杀”技术：大大降低了对用户计算机资源的占用，杀毒速度快速提升，无须升级即可查杀最新病毒。

（3）网购保护：在用户进行网上购物、支付、访问网银等操作时自动进行保护，防止黑客、木马病毒等问题对用户网上银行财产产生威胁，确保网购安全。

（4）智能、安全上网：通过智能反钓鱼、安全搜索、木马下载拦截、家长控制、ADSL 带宽管家等大量新增功能，保证用户安全上网、绿色上网、智能上网。

（5）体积小、资源小、高效升级：安装包体积小、杀毒速度快速提升、对系统影响小，升级时只下载几 KB 的文件，减小带宽占用。

瑞星杀毒软件 2012 具有 5 大高效杀毒技术，分别介绍如下。

（1）瑞星变频杀毒技术：智能检测计算机资源占用，自动分配杀毒时占用的系统资源，既保障电脑正常使用，又保证电脑安全。

（2）瑞星“云查杀”技术：大大降低用户计算机资源占用，杀毒速度快速提升，无须升级即可查杀最新病毒。

（3）高性能的反病毒虚拟机技术：快速准确查杀未知木马、未知病毒。

（4）高性能的木马病毒检测技术：查杀病毒时对系统资源占用小，速度大幅度提升。

（5）启发式病毒检测技术：准确查杀最新未知木马、病毒，有效解决采用最新技术的恶性病毒破坏系统。

7.4.2　金山杀毒软件

金山公司是国内著名的软件公司，其开发的金山毒霸对查毒速度做了优化，可以快速、彻底地查杀多种流行病毒。

金山毒霸 2012 极速轻巧，安装包不到 20MB，内存占用只有 19MB，首次扫描仅 4 分钟，3 分钟消灭活木马，扫描速度每秒可达 134 个文件。配合中国互联网最大云安全体系，100%鉴定文件是病毒还是正常文件。强大的自动分析鉴定体系使互联网上 95%的新未知文件，在 60 秒内即返回鉴定结果。应用精确样本收集技术更使文件鉴定准确率达到了 99%以上。

金山毒霸 2012 技术亮点如下。

（1）可信云查杀：增强互联网可信认证，海量样本自动分析鉴定，极速匹配查询，中国最大云安全，100%识别率，互联网 95%的新文件与未知文件 60 秒返回鉴定结果。

（2）蓝芯 II 云引擎 （BlueChipII CLOUD）：微特征识别（启发式查杀 2.0），将新病毒扼杀于摇篮中，针对类型病毒具有不同的算法，减少资源占用，多模式快速扫描匹配技术，超快样本匹配。

（3）白名单优先技术：准确标记用户计算机所有安全文件，无须逐一比对病毒库，大大提高了效率，双库双引擎，首家在杀毒软件中内置安全文件库，与可信云安全紧密结合，安全少误杀。

（4）个性功能体验：下载保护、聊天软件保护、U 盘病毒免疫防御、文件粉碎机、自定义安全区、提升性能、可定制的免打扰模式、自动调节资源占用、针对笔记本电源优化使续航更久。



7.4.3 江民杀毒软件

江民杀毒软件 KV2012 是全功能专业安全软件，全面融合杀毒软件、防火墙、安全检测、漏洞修复等核心安全功能为有机整体，打破杀毒软件、防火墙等专业软件各司其职的界限，为个人计算机用户提供了全面的安全防护。

江民杀毒软件 KV2012 秉承了江民杀毒软件一贯的尖端杀毒技术，更在易用性、人性化、资源占用方面取得了突破性进展。具有 9 大特色功能和 3 大创新安全防护，可以有效防御各种已知和未知病毒、黑客木马，保障计算机用户网上银行、网上证券、网上购物等网上财产的安全，杜绝各种木马病毒窃取用户账号、密码。

增强功能的江民安全专家，可以为系统优化加速，并可迅速扫描和查杀流行木马，清除流氓软件和恶意插件。其安全检测以及深层 Rootkit 隐藏病毒扫描功能，可以发现普通安全软件无法查出的深层安全隐患，进一步加固计算机系统的安全防线。

本 章 小 结

计算机病毒指编制的或者在计算机程序中插入的破坏计算机功能的数据、影响计算机使用并且能够自我复制的一组计算机指令或者程序代码，具有传染性、潜伏性、触发性和破坏性。计算机病毒可归纳为引导型病毒、可执行文件病毒、宏病毒、混合型病毒、特洛伊木马型病毒和 Web 网页病毒 6 种类型。

最后简单介绍了网络病毒的检测、防范和清杀方法以及常用的反病毒软件，如瑞星 2012 杀毒软件、金山杀毒软件和江民杀毒软件 KV2012。

习 题

一、填空题

1．计算机病毒的特征包括________、________、________、________。

2．计算机病毒可分为________、________、________、________、________和________ 6 种类型。

3．按照计算机病毒的传播媒介来分类，可分为________病毒和________病毒。

4．网络反病毒技术主要有 3 种，它们是预防病毒技术、________病毒技术和清除病毒技术。

5．宏病毒是指________。

二、选择题

1．计算机病毒是________。

A．一种程序　　B．传染病病毒
C．一种计算机硬件　　D．计算机系统软件

2．下列不属于计算机病毒特性的是________。
A．传染性　　B．突发性　　C．可预见性　　D．隐藏性

3．计算机病毒________。
A．都具有破坏性　　B．有些无破坏性
C．都破坏.exe 文件　　D．不破坏数据，只破坏文件

4．计算机病毒________。
A．是生产计算机硬件时不注意产生的　　B．都是人为制造的
C．都必须清除计算机才能使用　　D．有可能是人们无意中制造的

5．计算机病毒________。
A．破坏都是巨大的　　B．都具有可知性
C．只破坏计算机软件　　D．是可预防的

三、简答题

1．什么是计算机病毒？
2．计算机病毒的特征是什么？
3．计算机病毒可以分为哪几类？
4．简述网络病毒的清除方法。
5．计算机网络病毒的预防有哪几个方面？
6．简述计算机网络病毒的防治措施。

本章实训

实训　U 盘病毒工作原理及清除方法

实训目的

（1）了解 U 盘病毒的工作原理。
（2）掌握 U 盘病毒的清除方法。

实训环境

Windows XP/2000/2003，U 盘，计算器（或其他）程序。

实训原理

将一些病毒独立程序存放在移动存储设备中，并建立移动盘自动启用文件，当使用者打开移动存储设备时，自动启用文件引导病毒程序。

自动启用文件是微软公司为了方便用户而启动程序而设置的一种名为 autorun.inf 的文

本文件，位于移动盘的根目录，以纯文本的方式存放各种控制命令，用户双击盘符打开移动盘时就会自动打开并执行里面的命令。

如果自动启动文件被病毒所利用，当用户双击打开移动盘时就会自动启动病毒程序。

操作步骤

第 1 步：使用记事本或其他文本文件编辑软件，在 U 盘中建立名为 autorun.inf 的文本文件。

文件内容如下：

```
[autorun]                                              //这是自动启动文件固定格式
Shellexecute=c:\windows\system32\calc.exe;
//也可以是其他可执行程序或文档；下面内容不是必需的，是病毒采取的隐藏或迷惑用户的常用手法
icon=calc.exe                                          //更改移动盘图标为计算器
Label    计算器                                        //更改移动盘图标为计算器
Shell\计算器\Command=c:\windows\system32\calc.exe;  //在快捷菜单中添加计算器命令。
```

第 2 步：将上述文本文件以 autorun.inf 为文件名保存到 U 盘根目录。

第 3 步：重新输入 U 盘。

第 4 步：计算器自动启动。

第 5 步：U 盘病毒的清除方法。删除 autorun.inf 文件或格式化 U 盘即可。

第 8 章
黑客的攻击与防范

知识目标

- 理解黑客的概念、黑客的攻击目的。
- 了解黑客常用的攻击方法。
- 熟悉黑客常用攻击工具及攻击的防范。

技能目标

- 掌握防范黑客的技巧和方法。
- 掌握防范特洛伊木马的几种方法。

黑客是目前网络不安全的主要因素之一。了解黑客的行为以及攻击的方法，可以使我们加强网络安全的意识。黑客技术的发展，使网络安全成为网络设计与维护的重要内容，同时也促进了防范技术的发展。

8.1　什么是黑客

在网络世界里，黑客是指那些利用计算机的某些技术及其他手段恶意地进入其非授权范围以内的计算机或网络空间的人。360 安全中心发布的《2011 上半年中国网络安全报告》认为，2011 年上半年，黑客网络犯罪越来越多地瞄准人性弱点发起攻击：利用诱惑视频播放器、破解或改装软件，以及外挂软件捆绑传播的木马成为主流；同时，以低价购物、虚假中奖、博彩、股票欺诈为主的钓鱼欺诈网站数量持续猛增，相比去年同期增加近 5 倍，成为目前互联网的头号安全威胁。

目前，黑客的特征主要表现在以下几个方面。

1. 黑客群体扩大化

越来越多的人尤其是年轻人热衷于黑客技术，由于计算机和网络技术的普及，一大批没有受过系统的计算机和网络技术教育的黑客人才涌现出来。黑客群体中的绝大多数人是由好奇心驱使的黑客，这类黑客掌握较少的技术，使用现成的工具，攻击不设防的系统。还有少部分的黑客自己编写工具进行攻击，这部分黑客掌握着较好的技术，能够进入有所防备的系统，但是在一般情况下，他们有自己的道德观念和伦理文化，基本上不会有意破坏他人的系统和数据。第三部分特指极少数的被称为间谍的人，这类黑客是执着的进攻者，他们或因经济利益的关系，或因政治的原因，利用所掌握的技术或工具干扰被攻击系统的正常工作。

2. 黑客的组织化和集团化

目前，以前的那种以个人行为为主的黑客越来越少，被取而代之的是大批黑客组织。黑客组织化和集团化的优势是利用成员各自的不同特长进行合作攻击，从而提高攻击的成功率。

3. 黑客行为的商业化

大多数黑客把技术当作是谋生的手段。这些人一般在与网络技术相关的公司里工作，依靠自己高超的计算机和网络技术来设计、研制和管理安全产品。

4. 黑客行为的政治化

由于网络在人们的生产生活，尤其是国家军事安全中占有越来越重要的地位，致使网络安全可能会直接影响到国家安全。因此，各国政府都在准备迎接未来信息战争的挑战。相当多的黑客被政府部门雇用，去从事国家网络安全与攻击的研究。



8.2　黑客攻击的目的和步骤

1. 黑客攻击的目的和 3 个阶段

一般情况下，黑客的攻击总有明确的目的性。由于黑客们成长的经历和生活环境不同，其攻击目标也会多种多样，但大致上可以归纳总结如下。

（1）窃取信息。

黑客攻击最直接的目标就是窃取信息。黑客选取的攻击目标往往是许多重要的信息和数据，在获得这些信息与数据后，黑客就可以进行各种犯罪活动。政府、军事、邮电和金融网络是黑客攻击的首选目标。随着计算机与网络技术在政府、军事、金融、医疗、交通及电子等各个领域的广泛应用，黑客的各种破坏活动也随之猖獗。

窃取信息包括破坏信息的保密性和完整性。破坏信息的保密性是指黑客将窃取到的需要保密的信息发往公开的网站。而破坏信息的完整性是指黑客对重要文件进行修改、更换和删除，使得原来的信息发生了变化，以致于不真实或者错误的信息给用户带来了难以估量的损失。

事实上，获取口令也是窃取信息的一种，由于口令的特殊性，所以单独列出。黑客通过登录目标主机，或使用网络监听程序进行攻击。监听到口令后，就可以顺利地登录到其他主机，或者去访问一些本来无权访问的资源。

（2）控制中间站点。

在某些情况下，黑客登录目标主机后，不是为了窃取信息，只是运行一些程序，这些程序可能是无害的，仅仅消耗一些系统的处理时间。比如，黑客为了攻击一台主机，需要一个中间站点，以免暴露自己的真实所在。这样即便被发现，也只能找到中间站点的地址，而真正的攻击者可以隐藏起来。再比如，黑客不能直接访问某一严格受控制的站点或网络，此时就需要一个具有访问权限的中间站点，所以这个中间站点就成了首先要攻击的目标。

（3）获得超级用户权限。

黑客在攻击某一个系统时，都企图得到超级用户权限，这样就可以完全隐藏自己的行踪，并可在系统中埋伏下方便的后门，便于修改资源配置，做任何只有超级用户才能做的事情。

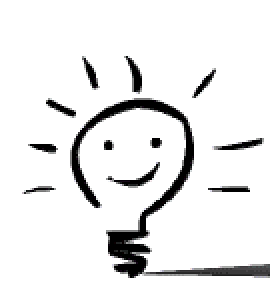
2. 黑客攻击可以分为 3 个阶段

（1）确定目标。

黑客进行攻击，首先要确定攻击目标。比如，某个具有特殊意义的站点、某个恶意的互联网服务提供商（ISP）、具有敌对观点的宣传站点或解雇了黑客的单位的主页等。

（2）收集信息。

收集信息的目的是为了进入所要攻击的目标网络的数据库。黑客会利用公开的协议或工具，收集驻留在网络系统中的各个主机系统的相关信息。



在黑客对特定的网络资源进行攻击前，他们需要了解将要攻击的环境，这需要搜集汇总各种与目标系统相关的信息，包括机器数目、类型、操作系统等。踩点和扫描的目的都是进行信息的搜集。

黑客搜集目标信息一般采用 7 个基本步骤，每一步均有可利用的工具，黑客使用它们得到攻击目标所需要的信息。

① 找到初始信息。

② 找到网络的地址范围。

③ 找到活动的机器。

④ 找到开放端口和入口点。

⑤ 弄清操作系统。

⑥ 弄清每个端口运行的是哪种服务。

⑦ 画出网络图。

（3）实施攻击。

黑客在搜集到相关信息后，就可以对目标系统实施攻击。黑客一旦获得了对攻击目标系统的访问权后，可有以下多种选择。

① 可能试图清除攻击入侵的痕迹，并在系统中建立另外的新的安全漏洞和后门，以使先前的攻击点被发现后，继续访问系统。

② 可能在目标系统中安装探测器软件，包括特洛伊木马程序，用来窥探所在系统的活动，收集黑客感兴趣的一切信息。

③ 可能进一步发现受损系统在网络中的信任等级，然后进一步通过该中间系统展开对整个系统的攻击。

④ 若黑客在受损系统上获得了特许访问权，就可以读取邮件、搜索和盗窃私人文件以及毁坏重要数据，从而破坏整个系统的信息，造成不堪设想的后果。

⑤ 黑客在攻击得手后，往往会继续在系统中寻找相关主机的可用信息，从而攻击其他系统。

8.3 黑客攻击方法

8.3.1 常见的黑客攻击方法

黑客的攻击手段多种多样，对常见攻击方法的了解将有助于用户达到有效防黑的目的。

1. 特洛伊木马攻击

特洛伊木马的攻击手段就是将一些“后门”、“特殊通道”隐藏在某个软件里，将使用该软件的计算机系统作为被攻击和控制的对象。特洛伊木马程序可以直接入侵用户的计算机并进行破坏，它常被伪装成工具程序或者游戏等，诱使用户打开带有特洛伊木马程序的邮件附件或从网上直接下载。一旦用户打开了这些邮件的附件或者执行了这些程序后，它



们就会留在用户的计算机中，并在系统中隐藏一个可以在 Windows 启动时悄悄执行的程序。当用户连接到 Internet 时，这个程序就会通知黑客，报告用户的 IP 地址以及预先设定的端口。黑客在收到这些信息后，再利用这个潜伏在其中的程序，就可以任意地修改用户的计算机的参数设定、复制文件、窥视用户整个硬盘中的内容等，从而达到控制用户计算机的目的。

2. Web 欺骗技术

欺骗是一种主动攻击技术，它能破坏两台计算机间通信链路上的正常数据流，并可能向通信链路上插入数据。一般 Web 欺骗使用两种技术，即 URL 地址重写技术和相关信息掩盖技术。首先黑客建立一个使人相信的 Web 站点的复制，它具有所有的页面和链接，然后利用 URL 地址重写技术，将自己的 Web 地址加在所有真实 URL 地址的前面。这样，当用户与站点进行数据通信时，就会毫无防备地进入黑客的服务器，用户的所有信息便处于黑客的监视之中了。但由于浏览器一般均有地址栏和状态栏，用户可以在地址栏和状态栏中获得连接中的 Web 站点地址及其相关的传输信息，并由此发现问题，所以黑客往往在 URL 地址重写的同时，还会利用相关信息掩盖技术，以达到掩盖欺骗的目的。

3. 口令攻击

口令攻击是指先得到目标主机上某个合法用户的账号后，再对合法用户口令进行破译，然后使用合法用户的账号和破译的口令登录到目标主机，对目标主机实施攻击活动。

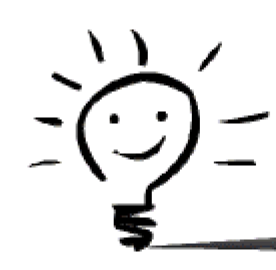
口令攻击方法获得用户账号的方法很多，主要是对口令的破译，常用的方法有以下几种。

（1）暴力破解。它基本上是一种被动攻击的方式。黑客在知道用户的账号后，利用一些专门的软件强行破解用户口令，这种方法不受网段限制，但需要有足够的耐心和时间，这些工具软件可以自动地从黑客字典中取出一个单词，作为用户的口令输入给远端的主机，申请进入系统。若口令错误，就按序取出下一个单词，进行下一个尝试，直到找到正确的口令或黑客字典的单词试完为止。由于这种破译过程是由计算机程序自动完成，因而几个小时内就可以把几十万条记录在字典里的所有单词都尝试一遍。

（2）密码探测。大多数情况下，操作系统保存和传送的密码都要经过一个加密处理的过程，完全看不出原始密码的模样，而且理论上要逆向还原密码的机率几乎为零。但黑客可以利用密码探测的工具，反复模拟编码过程，并将编出的密码与加密后的密码相比较，如果两者相同，就表示得到了正确的密码。

（3）网络监听。黑客可以通过网络监听得到用户口令，这类方法有一定的局限性，但危害性极大。由于很多网络协议根本就没有采用任何加密或身份认证技术，如在 Telnet、FTP、FTTP、SMTP 等传输协议中，用户账号和密码信息都是以明文形式传输的，此时若黑客利用数据包截取工具便可很容易收集到用户的账号和密码。另外，黑客有时还会利用软件和硬件工具时刻监视系统主机的工作，等待记录用户登录信息，从而取得用户密码。

（4）登录界面攻击法。黑客可以在被攻击的主机上，利用程序伪造一个登录界面，以骗取用户的账号和密码。当用户在这个伪造的界面上输入登录信息后，程序可将用户的输入信息记录并传送到黑客的主机，然后关闭界面，给出提示信息“系统故障”或“输入错



误”，要求用户重新输入。此时，假的登录程序自动结束，才会出现真正的登录界面。

4. 电子邮件攻击

电子邮件是互联网上运用得十分广泛的一种通信方式，但同时它也面临着巨大的安全风险。攻击者可以使用一些邮件炸弹软件向目标邮箱发送大量内容重复、无用的垃圾邮件，从而使目标邮箱被撑爆而无法使用。当垃圾邮件的发送流量特别大时，还可以造成邮件系统的瘫痪。另外，对于电子邮件的攻击还包括窃取和篡改邮件数据、伪造邮件、利用邮件传播计算机病毒等。

5. 网络监听

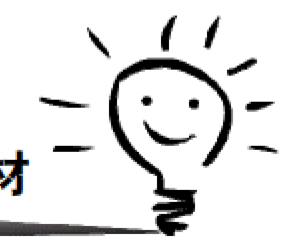
网络监听是主机的一种工作模式，在这种模式下，主机可以接收到本网段在同一物理通道上传输的所有信息，而不管这些信息的发送方和接收方是谁。网络监听可以在网上的任何一个位置进行，如局域网中的一台主机上、网关上、路由设备或交换设备上，或远程网的调制解调器之间等。因为系统在进行密码校验时，用户输入的密码需要求用户端传送到服务器端，这时，黑客就能在两端之间进行数据监听。此时若两台主机进行通信的信息没有加密，只要使用某些网络监听工具，就可轻而易举地截取包括口令和账号在内的信息资料。虽然网络监听获得的用户账号和口令具有一定的局限性，但黑客往往能够获得其所在网段的所有用户账号及口令。

6. 端口扫描攻击

所谓端口扫描，就是利用 Socket 编程与目标主机的某些端口建立 TCP 连接、进行传输协议的验证等，从而得知目标主机的扫描端口是否处于激活状态、主机提供了哪些服务、提供的服务中是否含有某些缺陷等。在 TCP/IP 协议中规定，计算机可以有 256×256 个端口，通过这些端口进行数据的传输。黑客一般会发送特洛伊木马程序，当用户不小心运行后，计算机内的某一端口就会打开，黑客就可通过这一端口进入用户的计算机系统。

7. 缓冲区溢出

许多系统都有这样或那样的安全漏洞，其中一些是操作系统或应用软件本身具有的，如缓冲区溢出攻击。缓冲区溢出是一个非常普遍、非常危险的漏洞，在各种操作系统、应用软件中广泛存在。产生缓冲区溢出的根本原因在于，将一个超过缓冲区长度的字串复制到缓冲区。溢出带来了两种后果，一是过长的字串覆盖了相邻的存储单元，引起程序运行失败，严重的可引起死机、系统重新启动等后果；二是利用这种漏洞可以执行任意指令，甚至可以取得系统特权。针对这些漏洞，黑客可以在长字符串中嵌入一段代码，并将过程的返回地址覆盖为这段代码的地址。当过程返回时，程序就转而开始执行这段黑客自编的代码了。一般说来，这段代码都是执行一个 Shell 程序。这样，当黑客入侵一个带有缓冲区溢出缺陷且具有 Suid-root 属性的程序时，就会获得一个具有 root 权限的 Shell，在这个 Shell 中黑客可以做任何事。恶意地利用缓冲区溢出漏洞进行攻击，可以导致程序运行失败、系统死机、重启等后果，更为严重的是，可以利用它执行非授权指令，甚至可以取得系统特权，进而进行各种非法操作，取得机器的控制权。



8.3.2　拒绝服务攻击

1. 拒绝服务攻击简介

拒绝服务（Denial of Service，DoS）攻击大致可以分为两类。一类是由于错误配置或者软件弱点导致的，某些 DoS 攻击是由于协议固有的缺陷或者对协议的实现导致的，这类攻击可以通过开发商发布简单的补丁来解决。另一类 DoS 攻击利用合理的服务请求来占用过多的服务资源，致使服务超载，无法响应其他的请求。这些服务资源包括网络带宽、文件系统空间容量、CPU 时间等。这种攻击会导致系统资源的匮乏。无论计算机的处理速度多快、内存容量多大、网络的带宽有多少，都总有一个极限，所以，总能找到一种方法使请求的值大于该极限值，对于这类攻击还没有一个固定的解决方案。

长期以来第一类 DoS 攻击，也就是由于错误配置或者软件弱点导致的攻击是攻击的主流方式。这是因为利用合理的服务请求来占用过多的服务资源，这种攻击方法往往需要相当大的带宽，而高带宽是大公司和国家科研机关所拥有的，以个人为主的黑客很难享用。为了克服这个缺点，攻击者开发出分布式攻击技术，利用工具集合许多的网络带宽来对同一个目标发送大量的请求，这就引入了一个新概念——分布式。这些程序可以使得分散在互联网各处的计算机共同完成对一台主机攻击的操作，从而使主机看起来好像是遇到了不同位置的许多主机的攻击。这些分散的计算机通过由几台主控制机来进行多种类型的攻击，如 UDP flood、SYN flood 等。

DoS 攻击的一个特点是这种攻击通常无法追踪。由于这种攻击一般不需要与目标之间的交互，所以攻击者可以伪造 IP 地址。在 UNIX 环境中伪造源 IP 地址非常容易，不过这需要攻击者具有 root 权限。

2. 常见的拒绝服务攻击

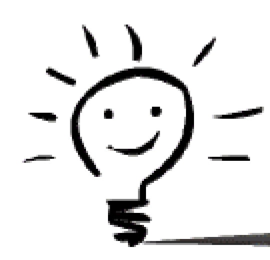
（1）flood。

flood 是“淹没”的意思，它是 DoS 攻击的一种手法，具有高带宽的计算机可以通过大量发送 TCP、UDP 或者 ICMP echo request 的报文，将低带宽的计算机“淹没”，降低对方计算机的响应速度。其中最简单的一种办法就是在 UNIX 下 ping 一个 IP，这种通过发送异常的、大的 ping 来杀掉服务器的方法有时称为 ping of death。另一种常用的手法称为 SYN flood，攻击者有意不完成 TCP 的 3 次握手过程，其目的是让等待建立某种特定服务的连接数量超过系统所能承受的数量，从而使得系统不能建立新的连接。

虽然所有的操作系统对每个连接都设置了一个计时器，如果计时器超时就释放资源，但是攻击者可以持续建立大量新的 SYN 连接来消耗系统资源。很显然，由于攻击者并不想完成 3 次握手过程，所以不需要接收 SYN / ACK，因此也就没有必要使用真实的 IP 地址。实现 SYN flood 是非常简单的，在互联网上有大量的源程序可以下载。

（2）Smurf。

Smurf 是一种很古老的 DoS 攻击，这种方法使用了广播地址（broadcast address）。发向广播地址的 IP 包会被网络中所有的计算机所接收，广播地址的尾数通常为 0，例如



192.168.1.0，尾数为 255 的地址通常作为多播地址（multicast address），但有时候也被用作广播地址。

设想发送一个 IP 包到广播地址 192.168.1.0，假设这个网络中有 50 台计算机，将会收到 50 次应答，广播地址在这里起到了放大器的作用，Smurf 攻击就利用了这种作用。如果 A 发送 1KB 大小的 ICMP echo request 到广播地址，那么 A 将收到 1KB×N 的 ICMP reply，其中 N 为网络中计算机的总数。当 N 等于 100 万时，产生的应答将达到 1GB，这将会大量消耗网络资源，如果 B 假冒了 A 的 IP 地址，那么收到应答的是 A，对 A 来说就是一次拒绝服务攻击。最经典的 Smurf 程序称为 parasmurf.c。

（3）短信拒绝服务攻击。

短信拒绝服务攻击是一种新型的移动终端的攻击手段，黑客通过计算机向目标发出巨量垃圾信息或指令，以致垃圾信息屏蔽了其他计算机的联网功能。

恶意黑客可采用与垃圾邮件相同的办法入侵流行的文本短信服务，从而使大都市的手机网络陷于瘫痪。黑客可构造各种的网络 post 表单、发包，从手机运营商向网络提供短信服务的方式看，这种攻击是可能的，因为这种方式也可使干扰短信系统的垃圾邮件发送者攻击手机语音网络，并使其瘫痪。

现如今多数的移动终端已经实现了智能化系统，市场中有大量关于拦截恶意骚扰的软件，一般此类软件可防御大部分的单端口攻击（单端口攻击：攻击者可通过多条线路来攻击同一终端，终端就会接收到多个号码的信息。单端口就是单一的号码，此类攻击可被一些防御软件拦截）。但如果攻击者通过多端口多线路攻击，此类的防御软件也就成了摆设，现如今常见的攻击中，多数可通过拦截号码与关键词的手段来防御，而对于特定的构造不同内容不同线路的攻击则无济于事。

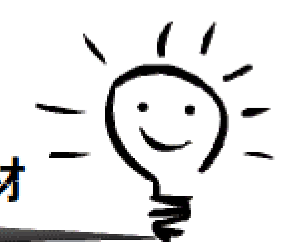
3. 拒绝服务攻击的防范方法

（1）用足够的机器承受黑客攻击。这是一种较为理想的应对策略。如果用户拥有足够的容量和足够的资源给黑客攻击，在它不断访问用户、夺取用户资源时，自己的能量也在逐渐耗失，或许未等用户被攻破，黑客就没有了后力。

（2）充分利用网络设备保护网络资源。所谓网络设备是指路由器、防火墙等负载均衡设备，它们可将网络有效地保护起来。当被攻击者被攻击时最先攻破的是路由器，但其他设备没有攻破。攻破的路由器经重启后会恢复正常，而且启动起来还很快，没有什么损失。若其他服务器被攻破，其中的数据会丢失，而且重启服务器又是一个漫长的过程，如果没有路由器这道屏障，被攻击者会受到无法估量的重创。

（3）使用 Inexpress、Express Forwarding 过滤不必要的服务和端口，即在路由器上过滤假 IP 地址。比如 Cisco 公司的 CEF（Cisco Express Forwarding）可以针对封包 Source IP 和 Routing Table 做比较，并加以过滤。

（4）使用 Unicast Reverse Path Forwarding 检查访问者的来源。它通过反向路由表查询的方法检查访问者的 IP 地址是否是真，如果是假的，它将予以屏蔽。许多黑客攻击常采用假 IP 地址方式迷惑用户，很难查出它来自何处，因此利用 Unicast Reverse Path Forwarding 可减少假 IP 地址的出现，有助于提高网络的安全性。



（5）过滤所有 RFC1918 IP 地址。RFC1918 IP 地址是内部网的 IP 地址，像 10.0.0.0、192.168.0.0 和 172.16.0.0，它们不是某个网段的固定 IP 地址，而是 Internet 内部保留的区域性 IP 地址，应该把它们过滤掉。

（6）限制 SYN/ICMP 流量。用户应在路由器上配置 SYN/ICMP 的最大流量来限制 SYN/ICMP 封包所能占有的最高频宽。这样，当出现大量的超过所限定的 SYN/ICMP 流量时，说明不是正常的网络访问，而是有黑客入侵。

8.3.3　特洛伊木马攻击

特洛伊木马，就是我们平常所说的木马，名称取自希腊神话特洛伊木马，它是一种基于远程控制的黑客工具，具有隐蔽性和非授权性的特点。这里的隐蔽性是指木马的设计者为了防止木马被发现，会采用多种手段隐藏木马，这样服务端即使发现感染了木马病毒，也很难确定其具体位置。非授权性是指控制端与服务端连接后，控制端将享有服务端的大部分操作权限，包括修改文件、修改注册表、控制鼠标和键盘等，而这些权力并不是服务端赋予的，而是通过木马程序窃取的。

从木马的发展来看，可以分为两个阶段。最初网络还处于以 UNIX 平台为主的时期，木马就产生了，当时木马程序的功能相对简单，往往是将一段程序嵌入到系统文件中，用跳转指令来执行一些木马的功能。这个时期木马的设计者和使用者大都是一些技术人员，具备了相当专业的网络和编程知识。后来，随着 Windows 平台的日益普及，一些基于图形操作的木马程序出现了，改善后的用户界面更加友好，使用者不需要懂得太多的专业知识就可以熟练地操作木马，木马的使用者增加了，相应的木马入侵事件也频繁出现了，而且由于这个时期木马的功能日趋完善，因此对服务端的破坏也更大了。

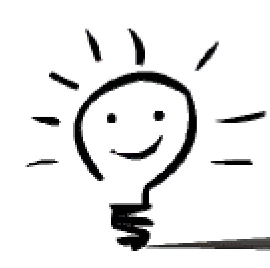
一个完整的木马系统由硬件、软件和具体连接部分组成。硬件部分是指建立木马连接所必须的硬件实体。前面曾经提到控制端和服务端，控制端指的是对服务端进行远程控制的一方；服务端是指被控制端远程控制的一方。而 Internet 则是控制端对服务端进行远程控制、传输数据的网络载体。软件部分是实现远程控制所必需的软件程序，包括控制端程序、木马程序以及木马配置程序。其中，控制端程序是控制端用以远程控制服务端的程序；木马程序是指潜入服务端内部，获取其操作权限的程序；木马配置程序是指设置木马程序的端口号、触发条件和木马名称等，这个程序主要是为了让木马在服务端更隐蔽。具体连接部分是指木马进行数据传输的目的地。

1. 配置木马

在这个阶段的主要目的是实现木马的伪装和信息反馈两个功能。木马的伪装是指为了更好地隐藏木马，采用多种伪装手段，如修改图标、捆绑文件或定制端口等诸多方式。信息反馈是指木马配置程序将信息反馈的方式或地址进行设置，比如设置信息反馈的邮件地址或 QQ 号等。

具体而言，木马的伪装形式包括以下几种。

（1）修改图标。用户在接收到的邮件的附件中看到文本文件的图标时，里面可能隐藏



着木马程序。因为现在已经有可以将木马服务端程序的图标改成.html、.txt 或.zip 等文件图标的专门技术。当然，目前提供这种功能的木马还不是很多，并且这种伪装也不是无懈可击的。

（2）捆绑文件。这种伪装手段是将木马捆绑在一个安装程序上，当安装程序运行时，木马在用户毫无察觉的情况下进入系统。

（3）出错提示。有一定木马知识的人都知道，如果打开一个文件，没有任何反应，这很可能就是个木马程序。木马的设计者为了弥补这个缺陷，就为木马提供了一个出错显示的功能。当服务端用户打开木马程序时，会弹出一个伪造的错误提示框，内容可以自定义，比如“文件无法打开!”之类的。

（4）定制端口。老式的木马程序所使用的端口一般都是固定的，利于判断是否感染木马。木马的设计者为了弥补这个缺陷，为木马提供了一个叫做定制端口的功能。控制端用户可以选择任意一个大于 1024 的端口作为木马端口，为判断木马带来了困难。

（5）自我销毁。当服务端打开含有木马的文件后，木马会将自己复制到操作系统的系统文件中。一般来说，原木马文件的大小和系统文件夹中的大小是一样的，感染了木马的用户只要在收到的邮件和下载的软件中找到原木马文件，在系统文件夹中找到相同大小的文件，就可以判断木马的存在了。而木马的自我销毁功能是指安装完木马后，原木马文件将自动销毁，这样服务端用户就很难找到木马的来源。

（6）木马更名。安装到系统文件夹中的木马的文件名一般是固定的，那么只要根据一定的常规知识，找到特定的文件，就可以知道中了什么木马。而现在有很多木马都允许控制端用户自由定制安装后的木马文件名，这样就很难判断所感染的木马类型了。

2. 传播木马

传播木马的方式主要有两种：一种是通过电子邮件，控制端将木马程序以附件的形式随同邮件发送；而另一种是软件下载，一些非正规的网站以提供软件下载的名义，将木马捆绑在软件安装程序上，程序下载后，只要一运行，木马就会自动安装。

3. 运行木马

木马自动安装后，首先将自己复制到操作系统的系统文件夹中，然后在注册表、启动组及非启动组中设置好木马的触发条件，这样木马的安装就完成了。安装后就可以启动木马了。木马的运行过程如下：设置木马的触发条件，木马进入内存，然后开启相应的端口。运行后的木马会将服务端的相关信息泄露给控制端，并在开放的端口等候控制端的连接。

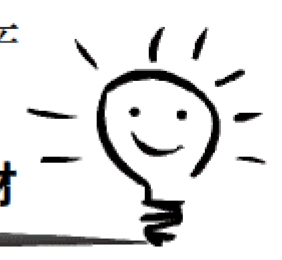
触发条件是指启动木马的条件，大致出现在以下几个地方。

（1）注册表[HKEY-LOCAL-MACHINE\Software\Microsoft\Windows\CurrentVersion\]的 Run 和 RunSerices 主键。

（2）system.ini 文件中在[386enh]、[mci]和[drivers32]内有关于启动木马的命令行。

（3）文件 autoexec.bat 和 config.sys 以及应用程序的启动配置文件也可以启动木马。这种加载方式一般都需要控制端用户与服务端建立连接后，将已添加木马启动命令的同名文件上传服务端覆盖这两个文件才行。

（4）注册表[HKEY-CLASSES-ROOT\文件类型\shell\open\command]主键。例如，国产



木马“冰河”就是修改此键，将“C:\Windows\SYSTEM\sysexplr.exe%1”改为“C：\Windows\system\sysexplr.exe%1”。双击一个文本文件后，原本应打开记事本的程序都变成启动木马的程序了。通过修改.html、.exe 及.zit 等文件的启动命令的键值可以启动木马。

（5）捆绑文件。实现这种触发条件要控制端和服务端已通过木马建立连接，然后控制端用户用工具软件将木马文件和某一应用程序捆绑在一起，上传到服务端覆盖文件。这样即使木马被删除了，只要运行捆绑了木马的应用程序，木马又会被运行安装。

（6）启动菜单。在“开始”→“程序”→“启动”选项下也可能有木马的触发条件。

木马运行时都在开放端口，如果在脱机状态下查看到有端口开放，或上网时，有一些数值比较大的端口开放，那就要小心查看是否已经感染了木马。

4. 信息泄露

设计成熟的木马都有信息反馈机制，这里的信息反馈是指木马成功安装后会收集一些服务端的软、硬件信息，并通过相关的方式反馈给控制端用户。泄露的信息包括操作系统、系统目录、硬盘分区情况和系统口令等。在这些信息中，最重要的是服务端的 IP 地址。因为控制端与服务端要建立连接，所以要得知服务端的 IP 地址及开放的端口号，而开放的端口是在木马程序中配置的，所以只有 IP 地址是控制端必得到的。控制端除了可以通过反馈得到外，还可以通过扫描开放特定端口的计算机的 IP 地址而获得。

5. 建立连接

有了 IP 地址后，木马连接就可以建立起来了，这样，控制端端口和木马端口之间就会出现一条通道。而控制端上的控制端程序就可以通过这条通道与服务端上的木马程序取得联系，并通过木马程序对服务端进行远程控制。

6. 远程控制

控制端能享有的控制权限有以下几种。

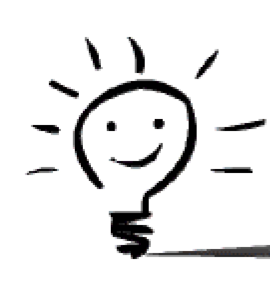
（1）窃取密码。一切以明文形式或缓存在 Cache 中的密码都能被木马侦测到，此外很多木马还提供按键记录功能，它将会记录服务端每次敲击键盘的动作。一旦木马入侵，用户密码将很容易被窃取。

（2）文件操作。控制端可由远程控制对服务端上的文件进行删除、新建、修改、上传、下载、运行和更改属性等一系列操作。

（3）修改注册表。控制端可任意修改服务端注册表，包括删除、新建或修改主键、子键或键值。这样，控制端就可以禁止服务端软驱和光驱的使用，锁住服务端的注册表，将服务端上木马的触发条件设置得更隐蔽，从而完成一系列高级操作。

（4）系统操作。这项内容包括重启或关闭服务端操作系统、断开服务端的网络连接、控制服务端的鼠标和键盘、监视服务端桌面操作、查看服务端进程以及控制端甚至可以随时给服务端发送信息。

随着网络的普及，上网的人或多或少都要受到木马的困扰。木马主要是通过下载软件和电子邮件两种途径传播。所以，为了避免感染木马，用户首先要到正规的网站去下载软件。然后，在接收邮件时，一定要谨慎地观察附件。如果附件是 EXE 文件或者是一些不常



见的文件类型，有可能是木马。另外，前面曾经提及木马也可以将图标伪装成.txt 或.html，这样就要看附件的长度了，一个木马程序一般都要 100KB 以上，而.txt 或.html 就不会这么大了。最后，就是看打开附件之后的反应了，如果打开附件毫无反应，或者是弹出一个出错提示框，那可能就是木马了。如图 8.1 所示为国产的木马程序“冰河”的客户端窗口。

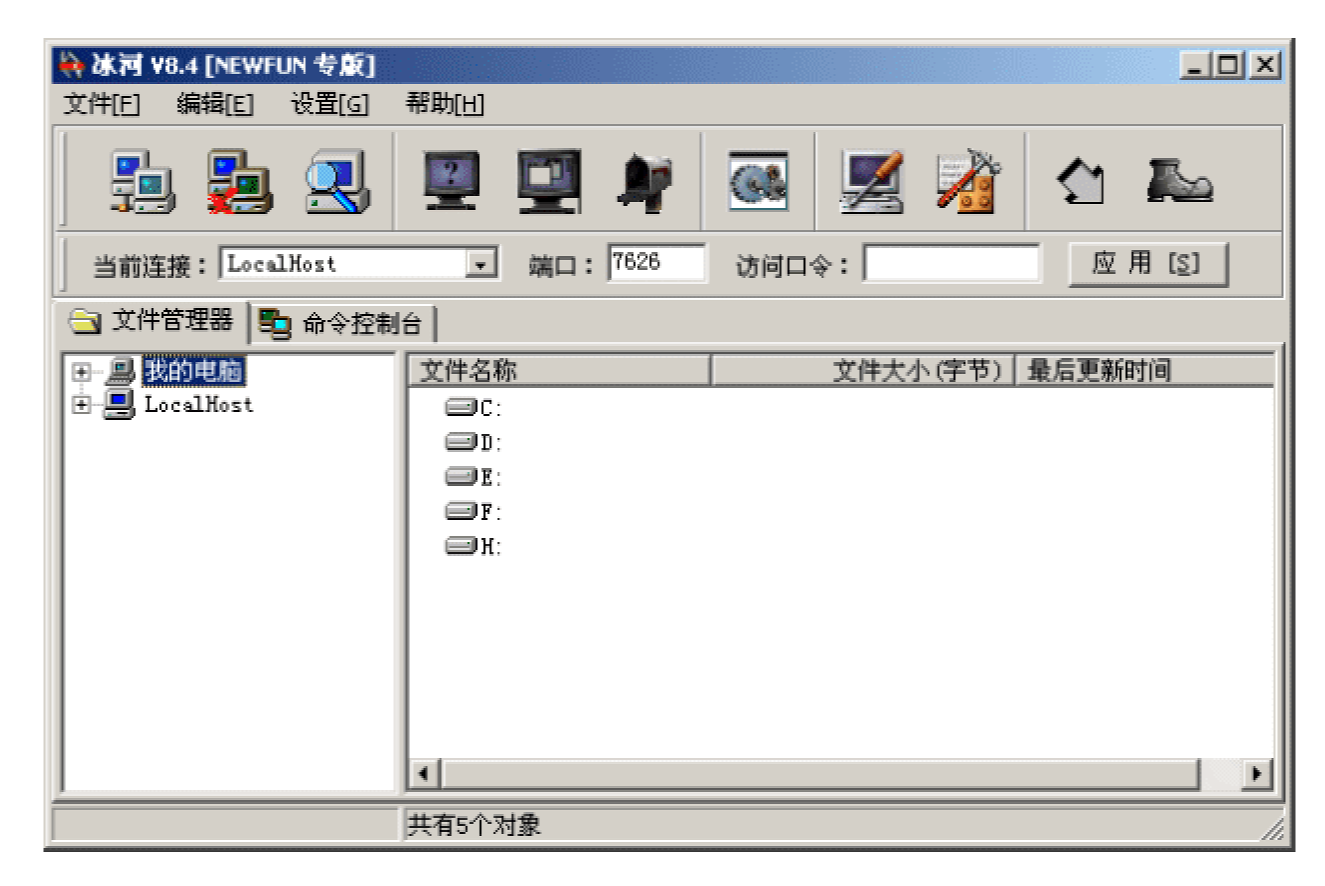


图 8.1　冰河 V 8.4 的客户端窗口

8.4　常见的黑客工具简介

8.4.1　邮件炸弹工具

所谓的邮件炸弹，指的是邮件发送者利用特殊的电子邮件软件，在很短的时间内连续不断地将邮件发送给同一个收信人，在这些数以千万计的大容量信件面前收件箱肯定不堪重负，而最终“爆炸身亡”。目前，知名的邮件炸弹有 Emailbomb、Kaboom3、Unabomb 等。

这种攻击手段不仅会干扰用户的电子邮件系统的正常使用，甚至它还能影响到邮件系统所在的服务器系统的安全，造成整个网络系统全部瘫痪，所以邮件炸弹具有很大的危害。

邮件炸弹可以大量消耗网络资源，常常导致网络塞车，使大量的用户不能正常地工作。通常，网络用户的信箱容量是很有限的，在有限的空间中，如果用户在短时间内收到上千上万封电子邮件，那么经过一轮邮件炸弹轰炸后的电子邮件的总容量很容易就把用户有限的阵地挤垮。这样用户的邮箱中将没有多余的空间接收新的邮件，那么新邮件将会被丢失或者被退回，这时用户的邮箱已经失去了作用；另外，这些邮件炸弹所携带的大容量信息不断在网络上来回传输，很容易堵塞带宽并不富裕的传输信道，这样会加重服务器的工作强度，减缓了处理其他用户的电子邮件的速度，从而导致了整个过程的延迟。

预防炸弹袭击的措施如下。

（1）向 ISP 求援。一旦信箱被轰炸了，但自己又没有好的办法来对付它，这时应该向你的 ISP 服务商求援，他们会采取办法帮你清除 Emailbomb。

（2）采用过滤功能。在邮件软件中安装一个过滤器（比如说 E-mail notify）是一种最有效的防范措施。在接收任何电子邮件之前预先检查发件人的资料，如果觉得有可疑之处，



可以将其删除，不让它进入用户的邮件系统。但这种做法有时会误删一些有用的邮件。如果担心有人恶意破坏你的信箱，给你发来一个“重磅炸弹”，你可以在邮件软件中启用过滤功能，把你的邮件服务器设置为有超过你信箱容量的大邮件时，自动进行删除。

（3）使用转信功能。有些邮件服务器为了提高服务质量往往设有“自动转信”功能，利用该功能可以在一定程度上解决容量特大邮件的攻击。假设用户申请了一个转信信箱，利用该信箱的转信功能和过滤功能，可以将那些不愿意看到的邮件统统过滤掉，删除在邮件服务器中，或者将垃圾邮件转移到自己其他免费的信箱中，或者干脆放弃使用被轰炸的邮箱，另外重新申请一个新的信箱。

（4）谨慎使用自动回信功能。所谓“自动回信”就是指对方给用户的这个信箱发来一封信而用户没有及时收取的话，邮件系统会按照用户事先的设定自动给发信人回复一封确认收到的信件。这个功能本来给大家带来了方便，但也有可能成为邮件炸弹。试想一下，如果给用户发信的人使用的邮件账号系统也开启了自动回信功能，那么当用户收到他发来的信而没有及时收取时，用户的系统就会给他自动发送一封确认信。恰巧他在这段时间也没有及时收取信件，那么他的系统又会自动给用户发送一封确认收到的信。如此一来，这种自动发送的确认信便会在双方的系统中不断重复发送，直到把用户双方的信箱都撑爆为止。

（5）用专用工具来对付。如果用户的邮箱不幸已经“中弹”，而且用户还想继续使用这个信箱名的话，可以用一些邮件工具软件（如 PoP-It）来清除这些垃圾信息。这些清除软件可以登录到邮件服务器上，使用其中的命令来删除不需要的邮件，保留有用的信件。

8.4.2　扫描工具

扫描工具是一种能够自动检测远程或本地主机安全弱点的程序，通过它可以获得远程计算机的各种端口分配及提供的服务和它们的版本。扫描器攻击时是通过选用不同的 TCP/IP 端口的服务，并记录目标主机给予的应答，以此搜集到关于目标主机的各种有用信息，而不是直接进攻，它获取的信息必须经过人为的分析才能成为真正有用的信息。当然，这需要用户具有一定的网络知识，否则，扫描器对于用户来说，将毫无用处。

下面介绍两种著名的扫描器。

1. 流光

流光是国内最著名的扫描、入侵工具，集端口扫描、字典工具、入侵工具、口令猜解等多种功能于一身，界面豪华，功能强大。它能让一个刚刚会用鼠标的人成为专业级黑客。它可以探测 POP3、FTP、SMTP、IMAP、SQL、IPC、IIS、FINGER 等各种漏洞，并针对各种漏洞设计不同的破解方案，能够在有漏洞的系统上轻易得到被探测的用户密码。流光对 Windows 9x/NT/2000 上的漏洞都可以探测，这使它成为了黑客手中必备的工具之一，其界面如图 8.2 所示。

流光的功能非常强大，它支持 163/169 双通和多线程检测，支持高效的用户流模式和高效服务器流模式，可同时对多台 POP3/FTP 主机进行检测，它支持最多 500 个线程控测，当线程超时时，阻塞线程具有自杀功能，不会影响其他线程。流光还支持 10 个字典同时检



测，并且检测设置可作为项目保存。



图 8.2 “流光”主界面

2. SuperScan

SuperScan 是一个功能强大的端口扫描工具。它可以通过 ping 来检验目标计算机是否在线，支持 IP 和域名相互转换，还可以检验一定范围内目标计算机的端口情况和提供的服务类别。SuperScan 可以自定义要检验的端口，并可以保存为端口列表文件，它还自带了一个端口列表，通过这个列表可以检测目标计算机是否有木马，同时用户也可以自己定义、修改以上木马端口列表。在 SuperScan 找到的主机上，单击鼠标右键可以实现 HTTP 浏览、Telnet 登录、FTP 上传、域名查询等功能，其界面如图 8.3 所示。

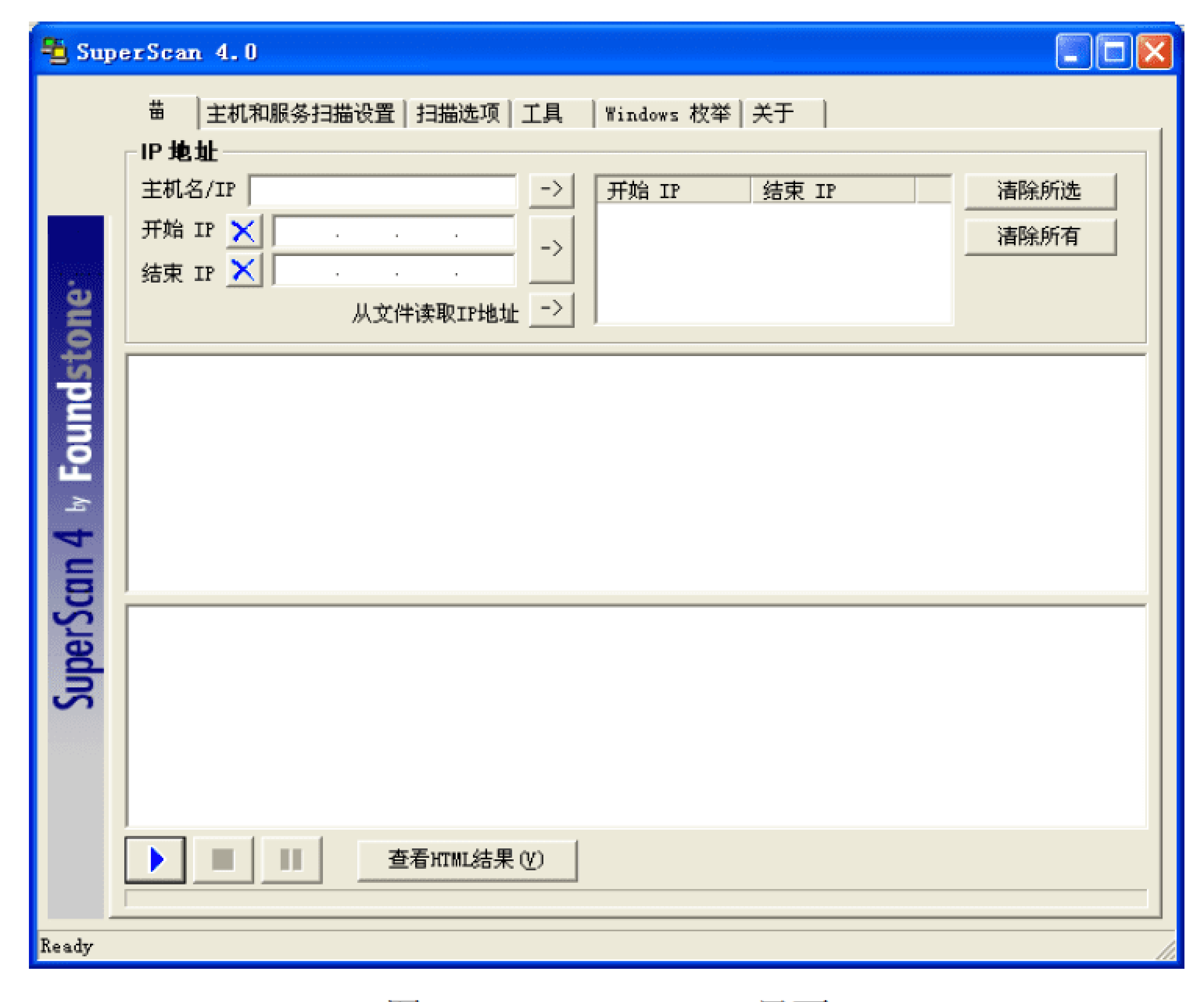


图 8.3 SuperScan 4.0 界面



SuperScan 扫描时的速度非常快，而且 CPU 占用率也非常小、非常平稳，甚至感觉不到它的运行。同时，SuperScan 扫描时占用的带宽也非常小，在使用宽带和电话拨号网络时，几乎没有什么差别。SuperScan 很适合扫描整个网段中的特定端口，用它做 1～65535 端口范围的扫描也非常适合，所以，许多人把 SuperScan 作为了扫描主机及制作 Sock 代理的必备工具。其缺点是扫描时，有些端口无法扫描到。

8.4.3　网络监听工具

网络监听是一种常用的被动式网络攻击方法，能帮助入侵者轻易获得用其他方法很难获得的信息，包括用户口令、账号、敏感数据、IP 地址、路由信息、TCP 套接字号等，是类似“食肉动物”一类的监听软件。一旦成功地登录目标网络上的一台主机，就会取得该机的超级用户权限，而且往往会尝试攻击网络中的其他主机，以实现对整个网络的监听。

网络监听通常在网络接口处截获计算机之间通信的数据流，是进行网络攻击最简单、最有效的方法。它具有以下特点：

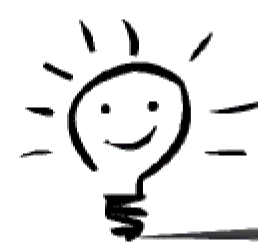
（1）隐蔽性强。进行网络监听的主机只是被动地接收网上传输的信息，没有任何主动的行为，既不修改网上传输的数据包，也不往链路上插入任何数据，很难被网络管理员觉察到。

（2）手段灵活。网络监听可以在网上的任何位置实施，可以是网上的一台主机、路由器，也可以是调制解调器。其中，网络监听效果最好的地方是在网络中某些具有战略意义的位置，如网关、路由器、防火墙之类的设备或重要网段；而使用最方便的地方是在网络中的一台主机上。

正因为网络监听具有以上特点，因此检测非常困难，这意味着更大的安全危害。虽然成功检测到网络监听的难度很大，但网络监听并非无懈可击，通过采取积极有效的措施，能够发现它的蛛丝马迹。

首先，监听非常消耗 CPU 资源。当系统运行网络监听软件时，系统因负荷过重，而对外界的响应很慢。因此，对于怀疑运行监听程序的主机，可用正确的 IP 地址和错误的物理地址去探测（如 Ping），运行监听程序的主机会有响应。这是因为正常的主机不接收错误的物理地址，而处于监听状态的主机能接收。另外，可向网上发送大量目的地址根本不存在的数据包，由于监听程序将处理这些数据包，会导致主机性能下降。通过比较该主机前后的性能，就可以作出判断，但这种方法难度较大。目前，有两个比较可行的办法：一是搜索网上所有主机运行的进程。网络管理员使用 UNIX 或 Windows NT 的主机，可以很容易地得到当前进程的清单，并确定是否有一个进程被从管理员主机上启动。二是搜查监听程序。现在监听程序只有有限的几种，管理员可以检查目录，找出监听程序。

还有两个方法在发现监听方面比较有效，但缺点也是难度较大：一是检查被怀疑主机中是否有一个随时间不断增长的文件存在，因为网络监听输出的文件通常很大，且随时间不断增长。二是通过运行 ipconfig 命令，检查网卡是否被设置成了监听模式；或使用 ifstatus 工具，定期检测网络接口是否处于监听状态。当网络接口处于监听状态时，很可能使入侵网络监听的防范比较困难，通常可采取数据加密和网络分段两种方法。



（1）数据加密。数据加密的优越性在于，即使攻击者获得了数据，如果不能破译，这些数据对他也是没有用的。一般而言，人们真正关心的是那些秘密数据的安全传输，使其不被监听和偷换。如果这些信息以明文的形式传输，就很容易被截获而且阅读出来。因此，对秘密数据进行加密传输是一个很好的办法。

（2）网络分段。即采用网络分段技术，建立安全的网络拓扑结构，将一个大的网络分成若干个小的网络，如将一个部门、一个办公室等可以相互信任的主机放在一个物理网段上，网段之间再通过网桥、交换机或路由器相连，实现相互隔离。这样，即使某个网段被监听了，网络中其他网段还是安全的。因为数据包只能在该子网的网段内被截获，网络中剩余的部分（不在同一网段的部分）则被保护了。

8.5 黑客攻击的防范

8.5.1 防止黑客攻击的措施

各种黑客的攻击程序虽然功能强大，但并不可怕。只要我们作好相应的防范工作，就可以大大降低被黑客攻击的可能性。具体来说，要做到以下几点。

1. 要提高安全意识

不随意打开来历不明的电子邮件及文件，不随便运行不太了解的人给的程序，防止运行黑客的服务器程序。尽量避免从 Internet 下载不知名的软件、游戏程序。即使从知名的网站下载的软件也要及时用最新的病毒和木马查杀工具对软件和系统进行扫描。密码设置尽量能使用字母数字混排，单纯的英文或者数字很容易被破解。常用的若干密码不应设置相同，防止被人查出一个，连带到重要的密码，并且密码最好经常更换。要及时下载并安装系统补丁程序。不随便运行黑客程序。

2. 使用反黑客软件

尽可能经常性地使用多种最新的、能够查解黑客的杀毒软件或可靠的反黑客软件来检查系统。必要时应在系统中安装具有实时检测、拦截、查解黑客攻击程序的工具。

3. 使用防火墙

防火墙是抵御黑客程序入侵的非常有效的手段。它通过在网络边界上建立起来的相应网络通信监控系统来隔离内部和外部网络，可阻挡外部网络的入侵和攻击。

4. 要安装杀毒软件

要将防毒、防黑当成日常例行工作，定时更新防毒组件，及时升级病毒库，将防毒软件保持在常驻状态，以彻底防毒。

5. 作好数据的备份

确保重要数据不被破坏的最好办法就是定期或不定期的备份数据，特别重要的数据应该每天备份。

6. 隐藏自己的 IP

保护自己的 IP 地址是很重要的。事实上，即便用户的机器上被安装了木马程序，若没有用户的 IP 地址，攻击者也是没有办法的，而保护 IP 地址的最好方法就是设置代理服务器。代理服务器能起到外部网络申请访问内部网络的中间转接作用，其功能类似于一个数据转发器，它主要控制哪些用户能访问哪些服务类型。

总之，我们应当认真制定有针对性的策略；明确安全对象，设置强有力的安全保障体系；在系统中层层设防，使每一层都成为一道关卡，从而让攻击者无缝可钻、无计可施。

8.5.2　发现黑客入侵后的对策

1. 估计受害形势，发出攻击警报

当确认系统受到入侵时，首先是尽可能快地估计入侵造成的破坏程度。当系统遇到严重破坏或不能正常运行时，向公安部门和信息安全部门报告，以便通过司法手段解决问题。

2. 采取措施

（1）杀死这个进程以切断黑客与系统的连接。必要时，切断网络连接，同时，注意保存现场，以便事后调查原因并进行分析。

（2）使用安全工具跟踪这个连接，找出黑客的来路和身份，询问他们究竟想要做什么，并发出警告。

（3）管理员可以使用一些工具来监视黑客，观察他们在做什么。

3. 使用网络工具

可以通过网络安全工具找到入侵者从哪个主机过来，然后查看哪些用户登录进入远程系统。

4. 修复漏洞

修复安全漏洞并恢复系统，不给黑客可乘之机。

本 章 小 结

黑客是指那些利用计算机的某些技术及其他手段，恶意地进入其非授权范围以内的计算机或网络空间的人。

黑客攻击的目的主要包括获取目标系统的非法访问、获取所需资料、篡改有关数据及利用有关资源。黑客的攻击手段包括特洛伊木马攻击、Web 欺骗、口令攻击、缓冲区溢出、端口扫描攻击等几种主要的方法。对常见攻击方法的了解，将有助于用户达到有效防黑的目的。

掌握常见的木马程序、扫描工具、破解工具、炸弹工具及安全防御工具的特点和使用方法，作好相应的防黑措施，设置强有力的安全保障体系，就可以大大降低被黑客攻击的可能性。



习　　题

一、填空题

1．通常黑客攻击的 3 个阶段是________、________和________。

2．常见的黑客攻击方法有________、________、________、________、________、________、________等。

3．特洛伊木马是一种黑客程序，它一般包括两个程序：一个是________；另一个是________。

4．传播木马的方式主要有两种：一种是通过________；另一种是________。

5．扫描工具是________的程序。

二、选择题

1．如果每次打开 Word 程序编辑文档时，计算机都会把文档传送到一台 FTP 服务器，那么可以怀疑 Word 程序已经被黑客植入________。

A．蠕虫　　B．FTP 程序　　C．特洛伊木马　　D．陷门

2．以下网络攻击中，________不属于主动攻击。

A．重放攻击　　B．拒绝服务攻击

C．通信量分析攻击　　D．假冒攻击

3．有一种攻击是不断对网络服务系统进行干扰，改变其正常的作业流程，执行无关程序使系统响应减慢甚至瘫痪。这种攻击叫做________。

A．重放攻击　　B．反射攻击　　C．拒绝服务攻击　　D．服务攻击

4．________不属于防止口令猜测的措施。

A．严格限定从一个给定的终端进行非法认证的次数

B．确保口令不在终端上再现

C．防止用户使用太短的口令

D．使用机器产生的口令

5．在网络安全中，窃取是指未授权的实体得到了资源的访问权，这是对________。

A．用性的攻击　　B．整性的攻击　　C．密性的攻击　　D．实性的攻击

三、简答题

1．什么是黑客？

2．黑客攻击的目的什么？

3．简述黑客攻击的步骤。

4．列举一些黑客攻击所采用的方法，并做简单分析。

5．常见的木马工具有哪些？它们是怎样运行的？
6．在使用计算机时，应采取哪些防黑措施？

本 章 实 训

实训 1　端口扫描软件 SuperScan 的使用

实训目的

（1）掌握端口扫描软件 SuperScan 的使用方法。
（2）掌握通过端口扫描软件发现、分析系统漏洞的能力。

实训环境

（1）连上 Internet 网络的一台计算机。
（2）端口扫描软件 SuperScan 4.0。

操作步骤

第 1 步：扫描 IP 地址。

下载并解压 SuperScan 4.0 后，双击 SuperScan.exe，开始安装。打开主界面，默认选择“扫描”（Scan）选项卡，允许用户输入一个或多个主机名或 IP 范围。也可以单击“从文件读取 IP 地址”按钮，从文件中选择输入地址列表。输入主机名或 IP 范围后，单击“开始扫描”按钮，SuperScan 将开始扫描地址，如图 8.4 所示。

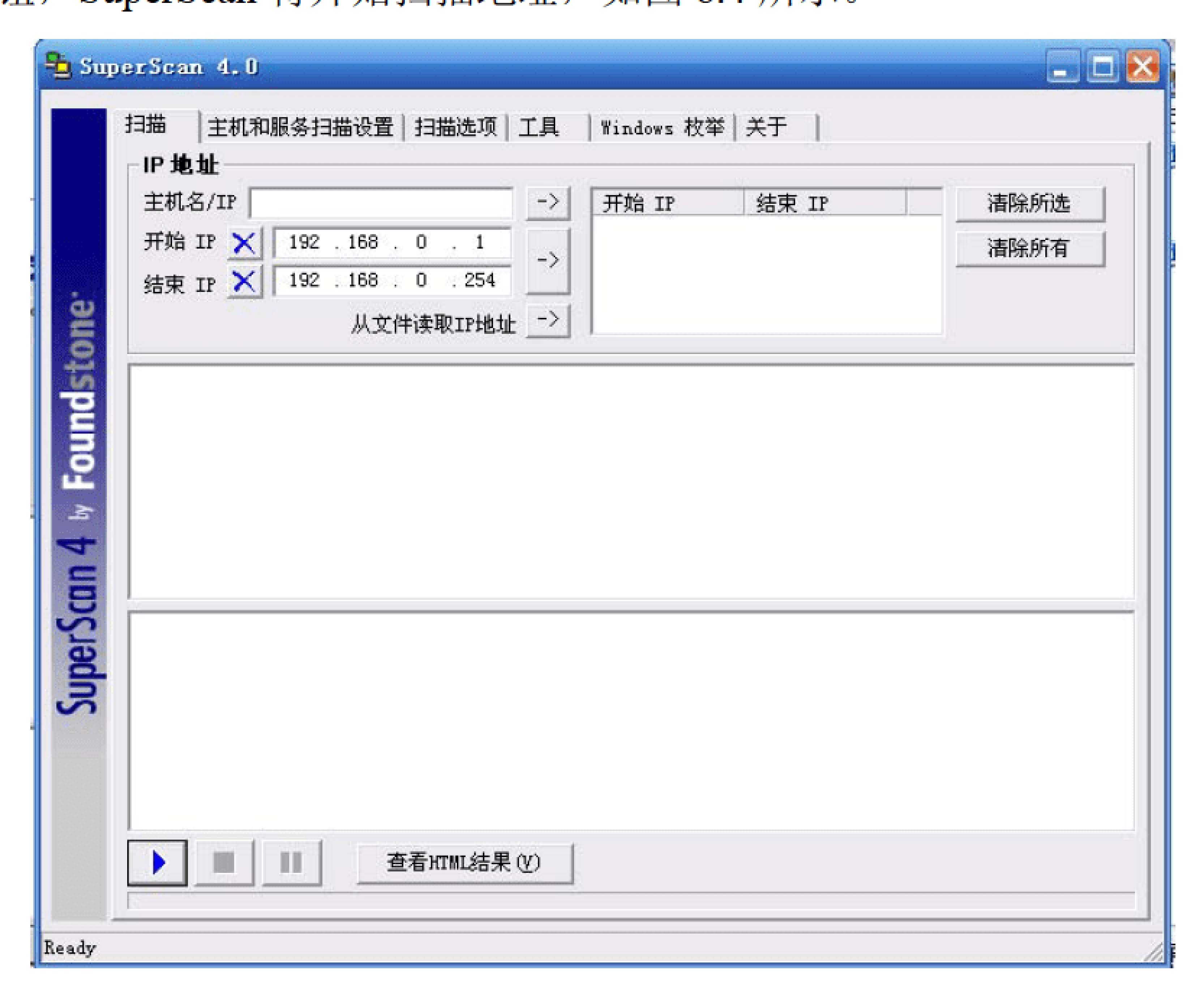


图 8.4　SuperScan 在指定的 IP 范围内扫描



扫描进程结束后，SuperScan 将提供一个主机列表，提供关于每台扫描过的主机被发现的开放端口的信息，如图 8.5 所示。SuperScan 还可以选择以 HTML 格式显示信息。

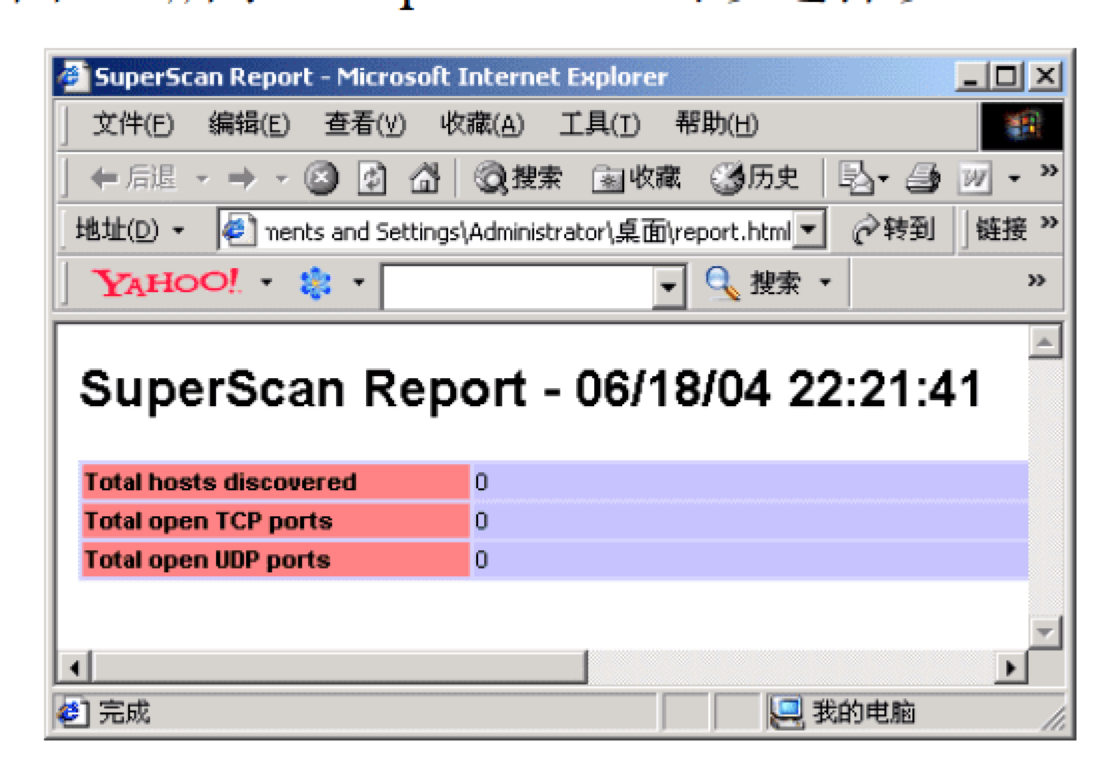


图 8.5　SuperScan 显示扫描了哪些主机和在每台主机上哪些端口是开放的

第 2 步：主机和服务器扫描设置。

步骤 1 是从一群主机中执行简单的扫描，然而很多时候需要定制扫描。此时应选择“主机和服务器扫描设置”选项卡，这个选项卡在扫描时可以看到更多信息，如图 8-6 所示。

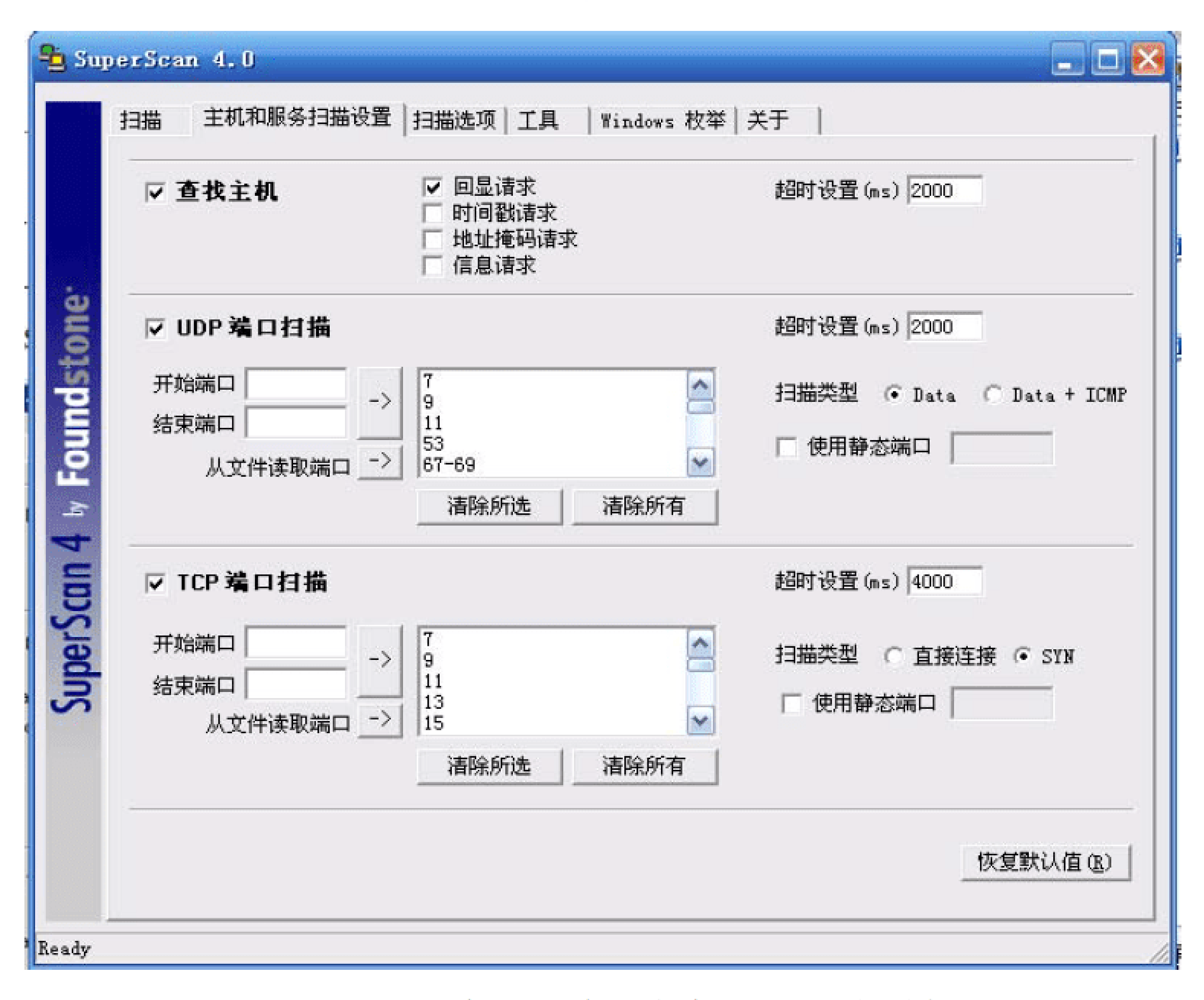


图 8.6　“主机和服务器扫描设置”选项卡

在选项卡顶部是“查找主机”选项，发现主机的默认方法是通过回显请求。通过选择和取消各种可选的扫描方式选项，也能够通过利用时间戳请求、地址掩码请求和信息请求来发现主机。应该注意的是，用户选择的选项越多，那么扫描所用的时间就越长。如果用户试图尽量多的收集一个明确的主机的信息，建议首先执行一次常规的扫描以发现主机，然后再利用可选的请求选项来扫描。在选项卡的下半部，包括“UDP 端口扫描”和“TCP 端口扫描”选项。通过屏幕的截图，注意到 SuperScan 最初开始扫描的仅仅是那几个最普

通的常用端口。原因是有超过 65000 个的 TCP 和 UDP 端口，若对每个可能开放端口的 IP 地址进行超过 130000 次的端口扫描，那将需要很长的时间。因此 SuperScan 最初开始扫描的仅仅是那几个最普通的常用端口，但给用户扫描额外端口的选项。

第 3 步：使用“扫描选项”（Scan Options）选项卡。

“扫描选项”选项卡允许进一步地控制扫描进程，如图 8.7 所示。选项卡中的首选项是定制扫描过程中主机和通过审查的服务数。1 是默认值，一般来说足够了，除非不太可靠。



图 8.7　“扫描选项”选项卡

接下来的“解析通过次数”选项，能够设置主机名解析的数量。同样，数量 1 足够了，除非用户的连接不可靠。另一个选项是“获取标志”的设置，“获取标志”是根据显示一些信息尝试得到远程主机的回应。默认的延迟是 8000ms，如果用户所连接的主机较慢，这个时间就显得不够长。

旁边的滑块是扫描速度调节选项，能够利用它来调节 SuperScan 在发送每个包时所要等待的时间。最快的扫描，当然是调节滑块为 0。可是，扫描速度设置为 0，有包溢出的潜在可能。如果用户担心由于 SuperScan 引起的过量包溢出，最好调慢 SuperScan 的扫描速度。

第 4 步：使用“工具”（Tools）选项卡。

使用 SuperScan 的“工具”（Tools）选项卡可以使用户很快地得到许多关于一个明确的主机信息。正确地输入主机名或者 IP 地址和默认的连接服务器，然后单击用户想要得到的相关信息的按钮。如用户 Ping 一台服务器或 traceroute 和发送一个 HTTP 请求，其界面如图 8.8 所示。

第 5 步：使用“Windows 枚举”选项卡。

最后的功能选项是“Windows 枚举”，就像用户猜测的一样，如果用户设法收集的信息是关于 Linux/UNIX 主机的，那该选项就没什么用。但若用户需要 Windows 主机的信息，它确实很方便。如图 8.9 所示，其能够提供从单个主机到用户群组，再到协议策略的所有信息。

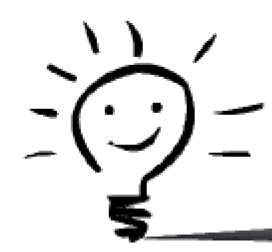




图 8.8 “工具”（Tools）选项卡

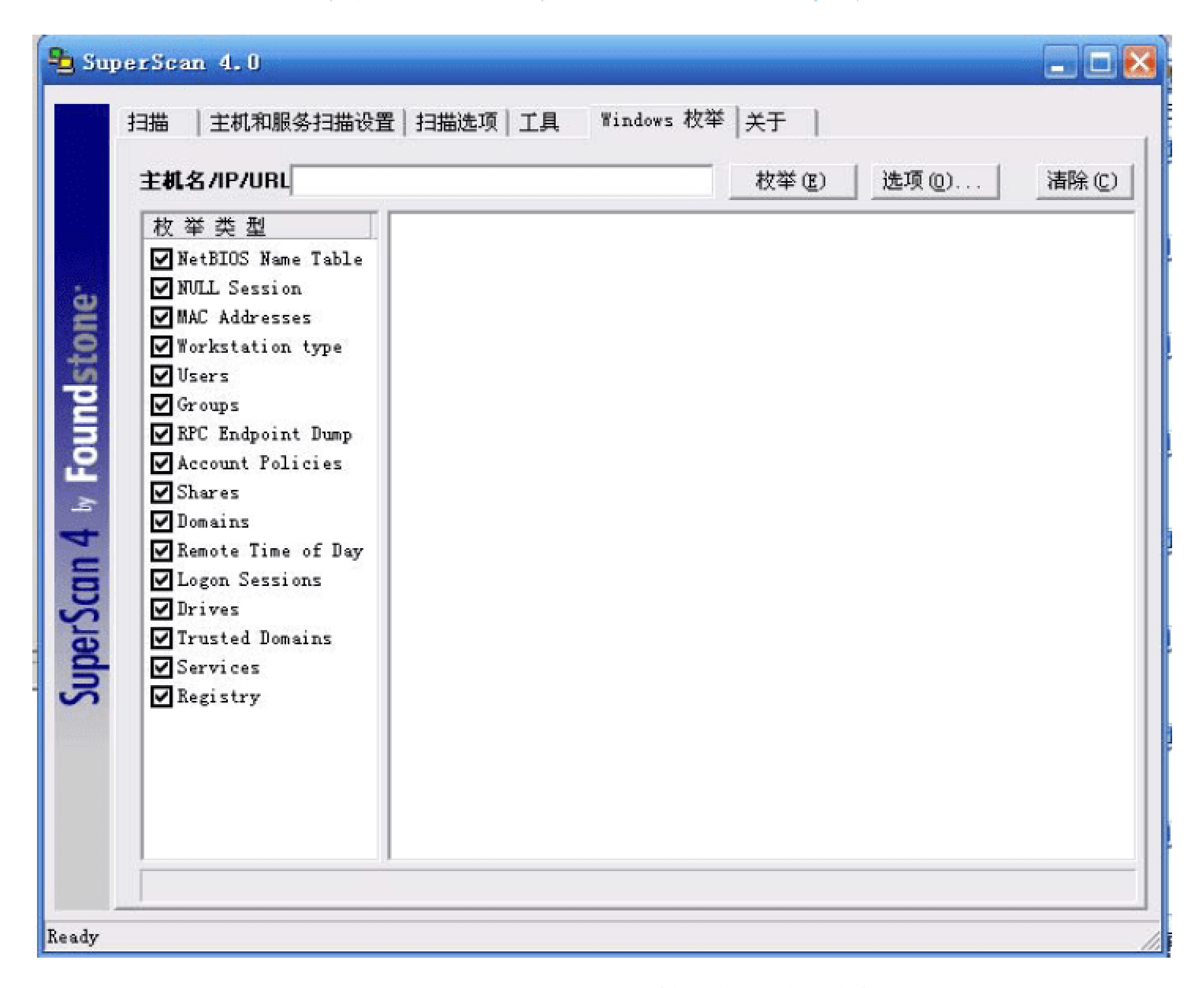


图 8.9 “Windows 枚举”选项卡

实训 2 冰河木马分析与清除

实训目的

（1）了解远程控制的基本原理。

（2）熟悉冰河木马的功能。

实训环境

（1）一台可以连上 Internet 的计算机。



（2）Windows XP/2000/2003 操作系统。

操作步骤

第 1 步：安装并控制远程目标。

安装冰河木马，并将冰河木马服务器端植入目标计算机。

第 2 步：跟踪目标。

通过服务器端自动跟踪目标机屏幕变化的同时可以完全模拟键盘及鼠标输入，即在同步被控端屏幕变化的同时，监控端的一切键盘及鼠标操作将反映在被控端屏幕上（局域网适用）。

第 3 步：记录各种口令信息。

其包括开机口令、屏保口令、各种共享资源口令及绝大多数在对话框中出现过的口令信息。

第 4 步：获取系统信息。

其包括计算机名、注册公司、当前用户、系统路径、操作系统版本、当前显示分辨率、物理及逻辑磁盘信息等多项系统数据。

第 5 步：远程文件操作。

其包括创建、上传、下载、复制、删除文件或目录、文件压缩、快速浏览文本文件、远程打开文件等多项文件操作功能。

第 6 步：注册表操作。

其包括对主键的浏览、增删、复制、重命名和对键值的读写等所有注册表操作功能。

第 7 步：发送信息。

以 4 种常用图标向被控端发送简短信息。

第 8 步：冰河木马的清除。

（1）冰河控制端可以自动卸载。

（2）手动清除方法：删除注册表中 Kernel32.exe 的键值；修改相关文本文件的关联；在 DOS 模式下将 Sysexplr.exe 和 Kernel32.exe 的隐藏属性改为只读，然后删除它们。



第 9 章 Web 安全与维护

知识目标

- 了解 HTTP 协议、HTML 语言。
- 熟悉服务器的安全策略。
- 熟悉浏览器、服务器的安全问题。

技能目标

- 熟练掌握 IE 浏览器的安全设置方法。
- 熟练掌握 Web 服务器的安全设置方法。

Web 作为 Internet 的一项重要的应用被广泛使用，它的安全性是必须要考虑的问题。

9.1　Web 概述

万维网（World Wide Web，WWW）是互联网上发展最快同时又使用最多的一项服务，它可以提供包括文本、图形、声音和视频等在内的多媒体信息。

万维网起源于 1989 年欧洲粒子物理研究所 CERN，其目的是收集时刻变化的报告、蓝图、绘制图、照片和其他文献。链接文档的万维网 Web 的最初计划是由 CERN 的物理学家 Tim Bermers-Lee 于 1989 年 3 月提出的，第一个原型（基于文本的）于 18 个月后运行。1991 年 12 月在德克萨斯州的圣安东尼奥（San Antonio）91 超文本会议上进行了一次公开演示，次年继续发展，并于 1993 年 2 月，在第一个图形界面 Mosaic 发布时达到了其发展的高峰。到今天 WWW 已经成了互联网上不可缺少的技术。

9.1.1　Web 简介

Web 是一种典型的分布式应用结构。Web 应用中的每一次信息交换都要涉及客户端和服务端。因此，Web 开发技术大体上也可以被分为客户端技术和服务端技术两大类。

WWW 由遍布互联网中的被称为 WWW 服务器（又称为 Web 服务器）的计算机组成。Web 是一个容纳各种类型信息的集合，从用户的角度看，万维网由庞大的、世界范围的文档集合而成，简称为页面。页面具有严格的格式，页面是用超文本标识语言（Hyper Text Markup Language，HTML）写成的，存放在 Web 服务器上。每一页面可以包含到世界上任何地方的其他相关页面的超链接（Hyperlink），这种能够指向其他页面的页称为超文本（Hypertext）。用户可以跟随一个超链接到其所指向的其他页面，并且这一过程可以被无限次的重复。通过这种方法可浏览无数互相链接的信息。

用户使用浏览器总是从访问某个主页开始的。由于主页中包含了超链接，因此可以指向另外的页面，这样就可以查看大量的信息。下面我们来看一下 WWW 中常用的一些术语及其意义。

1. 超文本标记语言（HTML）

HTML 是 ISO 标准 8879——标准通用标识语言（Standard Generalized Markup Language，SGML）在万维网上的应用。所谓标识语言就是格式化的语言，存在于 WWW 服务上的页，是用 HTML 描述的，它使用一些约定的标记对 WWW 的文字、图形、动画、声音、表格、链接、小游戏等进行描述。当用户浏览 WWW 上的信息时，浏览器会自动地解释这些标记的含义，并将其显示为用户在屏幕上所看到的网页。

一个 HTML 文本包括文件头（HEAD）和文件主体（BODY）两部分。其结构如下：

```
<HTML>
<HEAD>
```



```
</HEAD>
<BODY>
</BODY>
</HTML>
```

其中，<HTML>表示页的开始，</HTML>表示的页结束，它们是成对使用的；<HEAD>表示头的开始，</HEAD>表示头的结束；<BODY>表示主体的开始，</BODY>表示主体的结束，它们之间的内容才会在浏览器的正文中显示出来。HTML 的标识符有很多，用户可以查看有关网页制作方法的书籍进行了解。

2. 超文本传输协议（HTTP）

超文本传输协议（Hypertext Transfer Protocol，HTTP）是分布式、协作式、超媒体系统应用之间的通信协议，是万维网（World Wide Web）交换信息的基础。

它允许将超文本标记语言（HTML）文档从 Web 服务器传送到 Web 浏览器。HTML 是一种用于创建文档的标记语言，这些文档包含到相关信息的链接。用户可以单击一个链接来访问其他文档、图像或多媒体对象，并获得关于链接项的附加信息。

HTTP 工作在 TCP/IP 协议体系中的 TCP 协议上。

客户机和服务器必须都支持 HTTP，才能在万维网上发送和接收 HTML 文档并进行交互。

3. 统一资源定位器（URL）

统一资源定位器 URL（Uniform Resource Locator）是为了能够使客户端程序查询不同的信息资源时有统一访问方法而定义的一种地址标识方法。

万维网是以页面的形式来组织信息的。那么怎样来识别不同的页面、怎样才能知道页面在哪个位置，以及如何访问页面呢？为了解决这个问题，万维网采用了统一资源定位器 URL 的方法。

URL 是在互联网上唯一确定资源位置的方法，其基本格式如下：

协议：//主机域名/资源文件名

其中，协议（Protocal）用来指明资源类型，除了万维网用的 HTTP 协议外，还可以是 FTP、TELNET 等；主机域名表示资源所在机器的 DNS 名字；资源文件名用以提出资源在所在机器上的位置，包含路径和文件名，通常是“目录名/目录名/文件名”，也可以不含路径。例如，新浪网的 WWW 主页的 URL 就表示为：http://www.sina.com.cn/index.htm。

在输入 URL 时，资源类型和服务器地址不分字母的大小写，但目录和文件名则可能区分字母的大小写。这是因为大多数服务器安装了 UNIX 操作系统，而 UNIX 的文件系统是区分文件名大小写的。

9.1.2 Web 服务器

Web 服务器也称为 WWW 服务器，主要功能是提供网上信息浏览服务。



Web 服务器是一种被动程序，只有当 Internet 上运行在其他计算机中的浏览器发出请求时，服务器才会响应。

最常用的 Web 服务器是 Apache 和 Microsoft 的 Internet 信息服务器(Internet Information Server，IIS)。

Internet 上的服务器也称为 Web 服务器，是一台在 Internet 上具有独立 IP 地址的计算机，可以向 Internet 上的客户机提供 WWW、E-mail 和 FTP 等各种 Internet 服务。

9.1.3　Web 浏览器

Web 浏览器是阅读 Web 上信息的客户端的软件。如果用户在本地机器上安装了 Web 浏览器软件，就可以读取 Web 上的信息了。

Web 浏览器在网络上与 Web 服务器打交道，从服务器上下载和获取文件。Web 浏览器有多种，它们都可以浏览 Web 上的内容，只不过所支持的协议标准以及功能特性各有异同罢了。绝大部分的浏览器都运用了图形用户界面。目前常用的 Web 浏览器包括 Microsoft Internet Explorer、Netscape Navigator、Netscape Communicator、Opera、Mosaic、Lynx 等。

9.2　Web 的安全风险

9.2.1　Web 的安全体系结构

Web 的安全有很多因素需要考虑，如 Web 服务器的安全、Web 服务器所在的网络安全、Web 浏览器的无辜用户的安全风险等。

Web 赖以生存的环境包括计算机硬件、操作系统、计算机网络及相应的网络服务和应用，所有这些都存在着安全隐患，最终威胁到 Web 的安全。Web 的安全体系结构非常复杂，主要包括以下几个方面。

（1）客户端软件（即 Web 浏览器软件）的安全。

（2）运行浏览器的计算机设备及其操作系统的安全（主机系统的安全）。

（3）客户端的局域网（LAN）。

（4）Internet。

（5）服务器端的局域网（LAN）。

（6）服务器端的计算机设备及操作系统的安全（主机系统的安全）。

（7）服务器上的 Web 服务器软件。

在分析 Web 服务器的安全性时，要充分考虑上述影响 Web 服务器安全性的几个方面，其中安全性最差的将决定 Web 服务器的安全级别。影响 Web 安全的最直接的因素主要是 Web 服务器软件及支撑服务器运行的操作系统的安全。



9.2.2　Web 服务器的安全风险

现在，随着开放系统的发展和 Internet 的延伸，技术间的交流变得越来越容易，同时，人们也更容易获取功能强大的攻击安全系统的工具软件；另一方面，由于人才流动频繁，掌握系统安全情况的有关人员可能会成为无关人员，从而使得系统安全秘密的扩散成为可能。

Web 服务器的安全风险，主要来自以下几个方面。

（1）能否保证公布信息的真实、完整。维护公布信息的真实性和完整性是 Web 服务器最基本的要求。Web 服务器在一定程度上是站点拥有者的代言人，代表拥有者的形象。如果公布的信息被人篡改，可能会使信息遭到破坏，无法实现真正的提供信息的服务，甚至会加剧用户和站点拥有者的矛盾或者影响站点的形象。

（2）Web 服务能否安全可用。由于系统本身可能出现的问题以及他人的恶意破坏，可能会造成用户不能够获得 Web 服务，或者不能保证 Web 的服务确实有效；另一方面，需要保证所提供的服务是可信的，尤其是金融或者电子商务的站点。

（3）能否很好地保证 Web 访问者的隐私。要想取得用户的信赖，使其放心使用 Web 服务器的前提，首先要保护 Web 访问者的隐私。服务器上一般保留着用户的个人信息，诸如用户 IP 地址、电子邮件地址、所用计算机名称、单位名称、计算机简单说明、所访问页面内容、访问时间、传输数据量，甚至个人的信用卡号码等信息。一般情况下，用户不希望自己的隐私被别人发现甚至利用。

（4）Web 服务器可能会被入侵者作为“跳板”使用。Web 服务器最基本的要求是保护自己和 Web 浏览器用户。但常有非法入侵者将 Web 服务器作为“跳板”使用来进一步入侵内部网络或进一步危害其他网络。

9.2.3　Web 浏览器的安全风险

Web 浏览器为用户提供了一个功能强大、简单实用的图形化的界面，使用户不必经过专业化训练就可轻松自如地在网络的海洋里冲浪。它是目前网络上应用最多的工具之一。

但使用 Web 浏览器获取信息时，也是有安全风险的，主要有浏览器 URL 地址栏欺骗攻击、浏览器 URL 状态栏欺骗攻击、浏览器页面标签欺骗攻击、浏览器页面解析欺骗攻击、浏览器插件安全、浏览器本地存储安全、浏览器安全策略被绕过、浏览器隐私安全、浏览器差异等带来的安全风险。

例如，某浏览器的用户单击鼠标，想要看看新闻，查找一下资料，浏览一下某公司的主页，当一张张精彩的网页出现在计算机屏幕上时，同时，浏览器程序可能已经把某些信息传送给网络上的某一台计算机，这台计算机可能在世界的另一个角落。网页通过网络传到浏览器计算机中时，传来的内容有的是浏览器用户需要的、能够看到的，但是同时还有浏览器不能显示的内容，悄悄地存入浏览器计算机的硬盘上，这些不显示的内容，可能是协议工作内容，对用户是透明的，但是也可能是恶作剧代码，或者是蓄意破坏的代码，它

们会窃取 Web 浏览器用户计算机上的所有可能的隐私，也可能破坏计算机的设备，可能使用户在上网时误入歧途。因此，Web 浏览器也是有安全风险的。

9.3　Web 浏览器的安全

如果所有的网络用户都能够安分地使用网络这个美好的工具，那么 Web 浏览器用户就没有什么可以担忧的了，但非常不幸的是，网络世界是良莠不齐、复杂多样的，可能随时会受到恶意的攻击甚至被毁坏。

9.3.1　浏览器本身的漏洞

浏览器的功能越来越强大，但是由于程序结构的复杂，在堵住了旧漏洞的同时，可能又出现了新的漏洞。浏览器的安全漏洞可能让攻击者获取磁盘信息、安全口令，甚至破坏磁盘文件系统等。下面举出两个已知的浏览器安全漏洞。

1. UNIX 下的 Lynx 的一个安全漏洞

在 Lynx 的 2.7.1 版本之前，都存在着漏洞，只要做一个包含 backtick 字符的 LynxDownLoadURL，它就允许 Web 创建者在用户的机器上执行任意的命令。解决这个问题的方法是升级 Lynx 的版本。

2. Internet Explorer 的安全威胁

在这个浏览器中存在着许多安全威胁。

（1）远程执行代码漏洞。

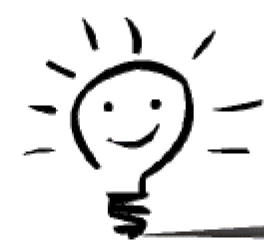
Internet Explorer 8、9 版本在访问内存中已被删除或尚未正确分配的对象的方式中存在一个远程执行代码漏洞。该漏洞可能以一种允许攻击者在 Internet Explorer 的当前用户的上下文中执行任意代码的方式损坏内存。攻击者可能拥有一个旨在通过 Internet Explorer 利用此漏洞的特制网站，然后诱使用户查看该网站。解决的方法就是安装补丁程序或者升级浏览器版本。

（2）拒绝服务漏洞。

Internet Explorer 8 处理恶意脚本代码时，远程攻击者可以利用漏洞使应用程序崩溃。通过构建恶意 Web 页，诱使用户访问，可触发此漏洞。

（3）地址栏 URI 欺骗漏洞。

在 Internet Explorer 8、9 版本代理服务设置中，如果 HTTP 和 Secure 栏中具有相同代理地址和端口，IE 没有确保 SSL 锁定图标与地址栏一致，通过特制的 HTML 文档触发多个任意主机的 HTTPS 请求，随后提交一个可信主机的 HTTPS 请求，再向不可信主机发送一个 HTTP 请求，可欺骗 Web 站点。



9.3.2 Web 页面中的恶意代码

由于某些动态页面以来源不可信的用户输入的数据为参数生成页面，所以 Web 页面中可能会不经意地包含一些恶意的脚本程序。如果 Web 服务器不对此进行处理，那么很可能对 Web 服务器和浏览器用户都带来安全威胁。即使采用 SSL 来保护传输，也不能阻止这些恶意代码的传输。

9.3.3 Web 欺骗

由于 Internet 上 Web 网页容易复制的特点，使得 Web 欺骗变得简单。

1. 欺骗攻击

所谓欺骗攻击就是指攻击者通过伪造一些容易引起错觉的文件、音像或者其他场景来诱导受骗者做出错误的与安全有关的决策。在网络虚拟的世界里，同样存在被骗的受害者。Web 欺骗就是一种网络欺骗，攻击者构建的虚假网站看起来就像真实站点，具有同样的连接，同样的页面，而实际上，被欺骗的所有浏览器用户与这些伪装的页面的交互都受到攻击者的控制。

2. Web 欺骗攻击的原理

Web 欺骗攻击成功的关键在于攻击者的伪服务器必须位于受骗用户到目标 Web 服务的必经路径上。

攻击者首先在某些 Web 网页上改写所有与目标 Web 站点有关的链接，使其不能指向真正的 Web 服务器，而是指向攻击者的伪服务器。当用户单击这些链接时，首先指向了伪服务器，攻击者向真正的服务器索取用户的所需界面。当获得目标 Web 送来的页面后，伪服务器改写链接并加入伪装代码，送给被欺骗的浏览器用户。

3. 对策

Web 欺骗攻击的危害大，上当的用户可能会不知不觉泄漏机密信息，还可能受到经济损失。为确保安全，用户可以采取以下的措施。

（1）尽量避免使用非有不可的浏览器的 JavaScript、ActiveX 和 Java 选项。

（2）充分利用浏览器的提示信息。

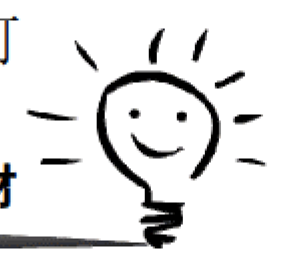
（3）进入 SSL 安全链接时，仔细查看站点的证书是否与其所声称的一致，不要被相似的字符欺骗。

9.4 Web 服务器的安全策略

9.4.1 制定安全策略

1. 定制安全政策

无论多么优秀的系统，必须有人进行安全管理和被合法地使用，否则，就没有安全可



言。所以，要有安全政策，它包括以下几个方面。

（1）定义安全资源，进行重要等级划分。

这是为了从全局的观点制定安全策略。它是一项具体的工作，不同单位、不同的管理层对安全资源的定义各不相同。

（2）进行安全风险评估。

安全风险评估是权衡考虑各类安全资源的价值和对它们保护所需要的费用，尽量以适当的开销获得满意的安全保障。很明显，个人娱乐站点的安全投资要比网上银行站点的安全投资少得多。

（3）制定安全策略的基本原则。

在安全资源的等级划分和风险评估的基础上，制定安全策略的基本原则。每个站点的基本策略都是独一无二的，它为该站点定义预期的安全级别，也就是说，该站点如何规划安全性。

（4）建立安全培训制度。

为增加单位员工的安全认识，从人为的角度尽量避免安全问题的发生，要建立安全培训制度。

（5）具有意外事件处理措施。

安全是相对的，不是绝对的。所以，必须明确无论安全措施如何完备、如何具体，还是有可能出现意外的安全问题，所以必须有相应的意外事件处理和补救的措施。

2. 认真组织 Web 服务器

服务器的安全策略有很多内容，这里简单介绍几个重要的内容：

- ☑ 选择好合适的 Web 服务器设备和相关软件。
- ☑ 提供静态页面和多种动态页面的能力。
- ☑ 接受和处理用户信息的能力。
- ☑ 提供站点搜索服务的能力。
- ☑ 远程管理的能力。

而关于安全方面的要求包括：

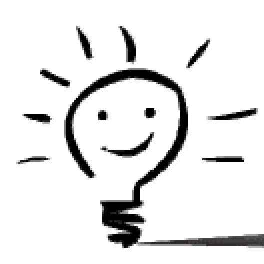
- ☑ 在已知的 Web 服务器漏洞中，针对该类型的漏洞最少。
- ☑ 对服务器的管理操作只能由授权用户执行。
- ☑ 拒绝通过 Web 访问不公开的信息。
- ☑ 能够禁止内嵌的不必要的网络服务。
- ☑ 能够控制各种形式的可执行程序的访问。
- ☑ 能够具有一定的容错性。
- ☑ 能对某些 Web 操作进行日志记录，便于执行入侵监测和入侵企图分析。

下面介绍 Web 服务器的配置和安全管理。

（1）仔细配置 Web 服务器。

因为服务器的重要性，在它的配置上，一定要仔细。一般采用如下方法。

① 将服务器与内部网隔离开。Web 服务器被入侵时，会造成 Web 服务器系统被破坏



甚至崩溃；入侵者收集如用户名、口令等信息；入侵者借助入侵的服务器为基础，进一步破坏其他网络等危害。

② 做好安全的 Web 站点的备份。备份系统是系统管理员必需做的一件事。通常，Web 服务器都采用多台备份机器在服务。但是要保证备份的内容是真实、可靠的和备份存储的地方是可靠、安全的。

③ 合理配置主机系统。主机的操作系统是 Web 的平台，合理地配置主机系统，能够为 Web 服务器提供强大的安全支持。主要考虑仅仅提供必要的服务和使用必要的辅助工具。

④ 合理配置 Web 服务器软件。

（2）Web 服务器的安全管理。

Web 服务器的安全管理主要包括以下几个方面。

① 更新 Web 服务器内容尽量采用安全方式，比如，尽可能的避免网络更新，而是采用本地方式。

② 经常审查有关日志。

③ 进行必要的数据备份。备份是对付任何意外事故的保留方法，是系统的最后的安全防线。

④ 定期对 Web 服务器进行安全检查。安全检查的目的是为了及时发现 Web 服务器系统的安全缺陷和及时发现入侵痕迹。

3. 了解最新的安全指南

了解最新的安全指南很重要，主要的目的有以下几点。

（1）及时更新系统软件和应用软件的版本，避免已存在漏洞的软件仍旧在使用。

（2）了解最新发现的安全漏洞和新的攻击工具的特点，以便做好预防。

（3）了解、掌握最新的安全保护技术和工具。

（4）修订原来的安全策略，引进必要的安全工具。

每个网站的安全需求不同，受到攻击的机率和手段都不相同，因此在实践中系统的安全工作要结合系统本身的特点来进行。

9.4.2 Web 服务器安全应用

1. 正确安装 Windows Server 2003

（1）分区和逻辑盘的分配。

推荐的安全配置是建立 3 个逻辑驱动器，第一个大于 2GB，用来装系统和重要的日志文件，第二个放 IIS，第三个放 FTP，这样无论 IIS 或 FTP 出了安全漏洞都不会直接影响到系统目录和系统文件。要知道，IIS 和 FTP 是对外服务的，比较容易出问题。而把 IIS 和 FTP 分开主要是为了防止入侵者上传程序并从 IIS 中运行。

（2）安装顺序的选择。

Windows Server 2003 在安装中有几个顺序是要注意的。

① 何时接入网络。Windows Server 2003 在安装时有一个漏洞，在输入密码后，系统



就建立了 ADMIN$的共享，但是并没有用刚刚输入的密码来保护它，这种情况一直持续到再次启动后，在此期间，任何人都可以通过 ADMIN$进入你的机器；同时，只要安装一完成，各种服务就会自动运行，而这时的服务器是满身漏洞，非常容易进入。因此，在完全安装并配置好 Windows Server 2003 前，一定不要把主机接入网络。

② 补丁的安装。补丁的安装应该在所有应用程序安装完之后，因为补丁程序往往要替换/修改某些系统文件，如果先安装补丁再安装应用程序有可能导致补丁不能起到应有的效果。

2. 安全配置 Windows Server 2003

即使正确地安装了 Windows Server 2003，系统还是有很多的漏洞，还需要进一步进行细致的配置。

（1）端口。它是计算机和外部网络相连的逻辑接口，也是计算机的第一道屏障，端口配置正确与否直接影响到主机的安全。一般来说，仅打开需要使用的端口会比较安全。配置的方法是在“网卡属性”→“TCP/IP”→“高级”→“选项”→“TCP/IP 筛选”选项中启用 TCP/IP 筛选，不过对于 Windows Server 2003 的端口过滤来说，有一个不好的特性：只能规定打开哪些端口，不能规定关闭哪些端口，这样对于需要打开大量端口的用户就不太方便。

（2）IIS。它是微软组件中漏洞最多的一个，平均两三个月就要出一个漏洞，而微软的 IIS 默认安装又不安全，所以 IIS 的配置是重点。

① 把 C 盘那个 Inetpub 目录彻底删掉，在 D 盘新建一个 Inetpub 文件，也可以给目录改一个名字，但是自己要记得，然后在 IIS 管理器中将主目录指向 D:\Inetpub。

② 将 IIS 安装时默认的 Scripts 等虚拟目录一概删除，如果需要什么权限的目录，再建立对应的目录。

3. 账号安全

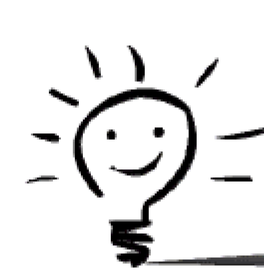
Windows Server 2003 的账号安全是另一个重点。首先，Windows Server 2003 的默认安装允许任何用户通过空用户得到系统所有账号/共享列表，这个本来是为了方便局域网用户共享文件的，但是一个远程用户也可以得到用户列表并使用暴力法破解用户密码。Windows Server 2003 的本地安全策略（如果是域服务器就是在域服务器安全和域安全策略中）有这样的选项——RestrictAnonymous（匿名连接的额外限制），该选项有 3 个值。

☑ 0：None. Rely on default permissions（无，取决于默认的权限）。

☑ 1：Do not allow enumeration of SAM accounts and shares（不允许枚举 SAM 账户和共享）。

☑ 2：No access without explicit anonymous permissions（没有显示匿名权限就不允许访问）。

值 0 是系统默认的，什么限制都没有，远程用户可以知道你计算机上所有的账户、组信息、共享目录、网络传输列表（NetServerTransportEnum）等，对服务器来说这样的设置非常危险。值 1 只允许非 NULL 用户存取 SAM 账户信息和共享信息。值 2 在 Windows Server 2003 中才支持，推荐设为 1 比较好。



这样，入侵者现在就没有办法拿到用户列表，应该说账户安全了。另外，为了安全还要将系统内建的 administrator 账户改名。

4. 设置好完全策略

设置策略和设置方法可参照 Windows Server 2003 网络安全与策略（第 4 章）这一部分的内容。

5. 目录和文件权限

为了控制好服务器上用户的权限，同时也为了预防以后可能的入侵和溢出，还必须非常小心地设置目录和文件的访问权限，NT 的访问权限包括读取、写入、读取及执行、修改、列目录和完全控制。在默认情况下，大多数的文件夹对所有用户（Everyone 这个组）是完全敞开的（Full Control），需要根据应用的需要进行权限重设。

实际上，Web 的安全和应用在很多时候是矛盾的，因此，需要在其中找到平衡点，毕竟服务器是给用户用而不是做 OPEN HACK 的，如果安全原则妨碍了系统应用，那么这个安全原则也不是一个好的原则。

网络安全是一项系统工程，它不仅有空间的跨度，还有时间的跨度。很多用户（包括部分系统管理员）认为进行了安全配置的主机就是安全的，其实这其中有个误区：我们只能说一台主机在一定的情况、一定的时间上是安全的，随着网络结构的变化，新的漏洞的发现，管理员/用户的操作，主机的安全状况是随时随地变化的，只有让安全意识和安全制度贯穿整个过程才能做到真正的安全。

本 章 小 结

Web 是一种典型的分布式应用结构。Web 开发技术被分为客户端技术和服务端技术两大类。

Web 的安全有很多因素需要考虑，如 Web 服务器的安全、Web 服务器所在的网络安全、Web 浏览器的用户的安全风险等。

习 题

一、填空题

1．WWW 服务采用客户机/服务器工作模式，它以________与超文本传输协议 HTTP 为基础，为用户提供界面一致的信息浏览系统。

2．HTTP 协议是分布式的 Web 应用的核心技术协议，在 TCP/IP 协议栈中属于______层协议。

3．目前常用的 Web 浏览器主要有________和________两种。

4．Web 浏览器的不安全因素主要来自________。



5．Web 欺骗攻击是指________。

二、选择题

1．在访问互联网过程中，为了防止 Web 页面中恶意代码对自己计算机的损害，可以采取________防范措施。

A．利用 SSL 访问 Web 站点

B．将要访问的 Web 站点按其可信度分配到浏览器的不同安全区域

C．在浏览器中安装数字证书

D．要求 Web 站点安装数字证书

2．统一的安全电子政务平台包括统一的可信 Web 服务平台、统一的 Web 门户平台与统一的________。

A．数据交换平台　B．电视会议平台　C．语音通信平台　D．电子邮件平台

三、简答题

1．Web 服务器的安全需求有哪些？

2．Web 浏览器的安全需求有哪些？

3．简述 Web 服务器的安全策略。

4．如何进行服务器的安全配置？

本 章 实 训

实训 1　IE 浏览器的安全设置

实训目的

（1）了解 IE 浏览器的基本功能。

（2）掌握提高 IE 浏览器安全性的设置方法。

实训环境

（1）一台连上 Internet 的计算机。

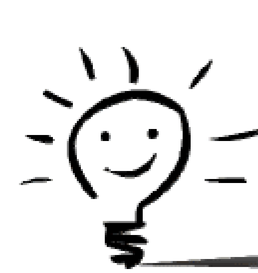
（2）IE 8.0 浏览器。

操作步骤

第 1 步：IE 浏览器安全性的设置。

有很多针对 IE 浏览器的病毒都是通过在网页中使用恶意脚本程序来运行的，只需要禁止在浏览器中执行这些脚本就可以达到防范于未然的目的。

在 IE 浏览器中选择“工具”→“Internet 选项”命令，即可打开“Internet 选项”对话框，如图 9.1 所示。选择“安全”选项卡，如图 9.2 所示。



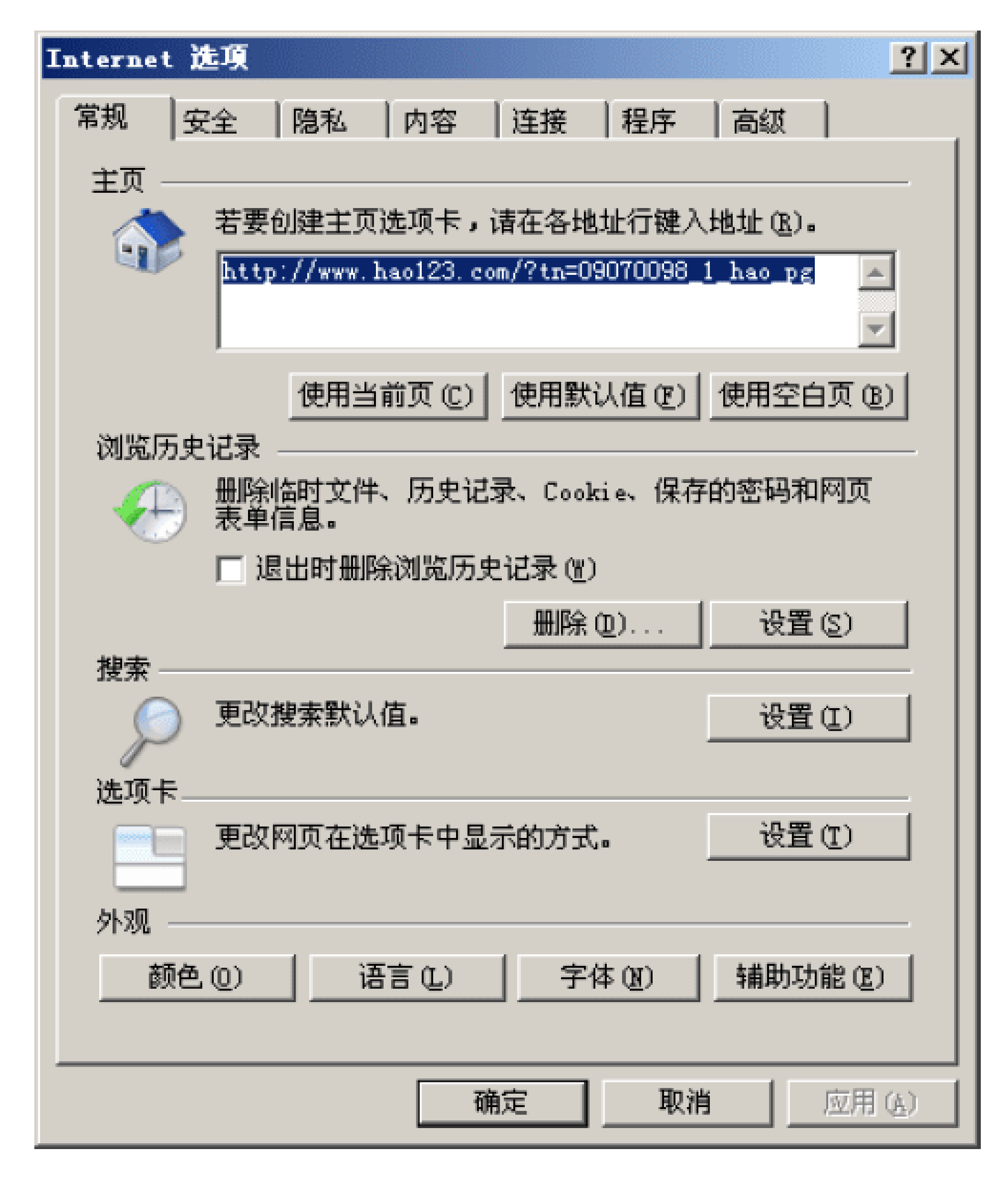




图 9.1 “Internet 选项”对话框



图 9.2 “安全”选项卡

在“安全”选项卡中单击“自定义级别”按钮，弹出“安全设置”对话框，如图 9.3 所示。将“脚本”选项中的“Java 小程序脚本”和“活动脚本”都设置成“禁用”，以便以后上网浏览时不用担心脚本类病毒。不过，正常网页中所有通过脚本实现的网页特殊效果也被禁用了。

第 2 步： 删除 Internet 临时文件。

在用户上网冲浪时，IE 会自动产生一些临时文件、垃圾文件和记录一些信息，在很多情况下这些痕迹也能暴露用户的隐私信息。

选择 IE 浏览器的“工具”→“Internet 选项”命令，打开“Internet 选项”对话框，选择“常规”选项卡，单击“删除”按钮。然后在弹出的“删除浏览的历史记录”对话框中选中“Internet 临时文件”复选框，单击“删除”按钮，如图 9.4 所示。

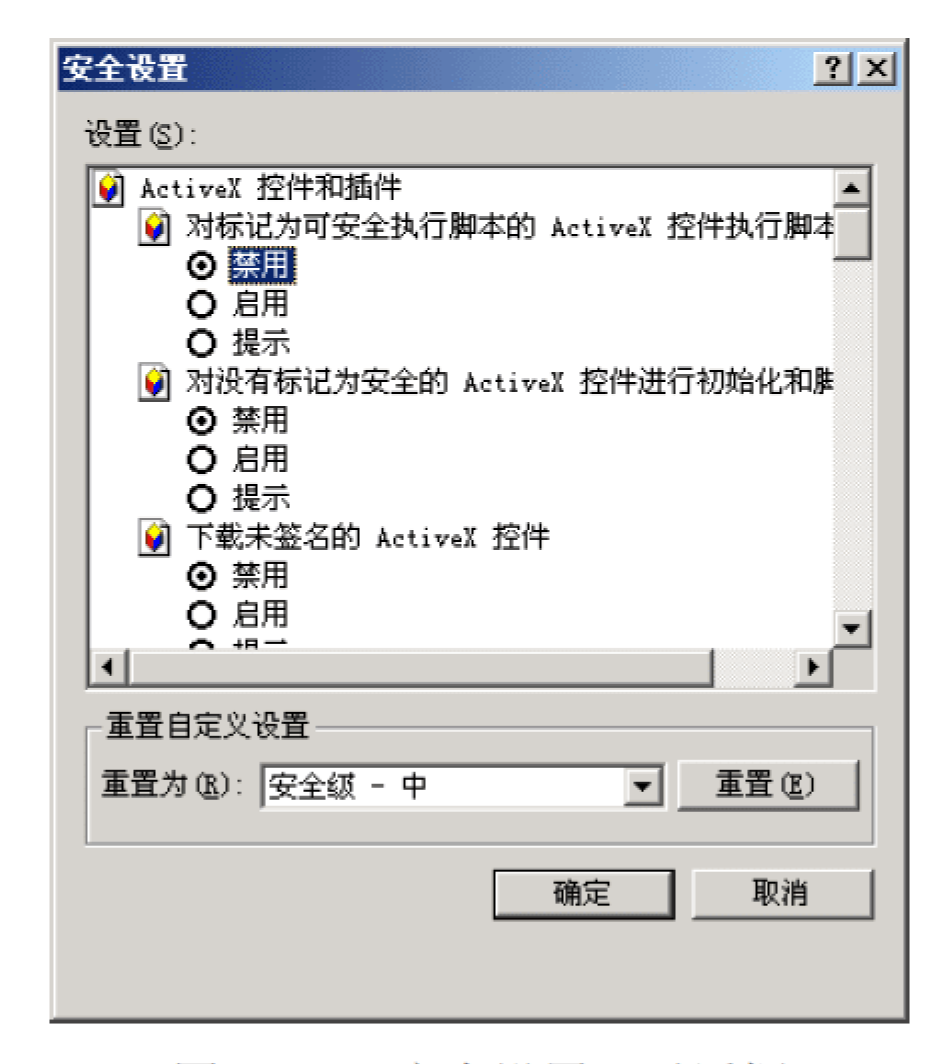


图 9.3 “安全设置”对话框

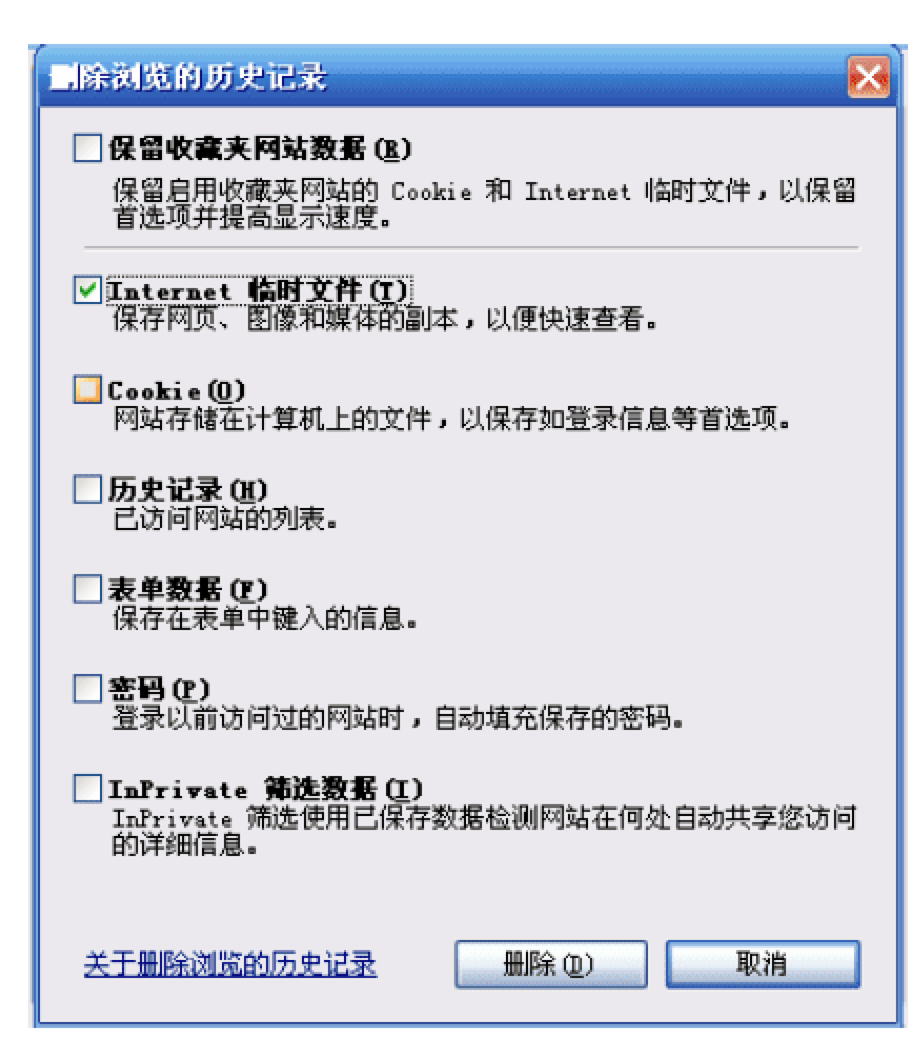
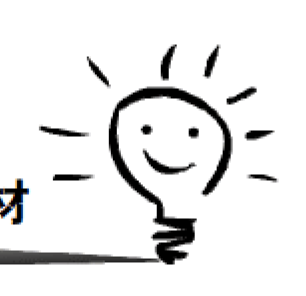


图 9.4 “删除浏览的历史记录”对话框



第 3 步：清除 IE 的历史记录。

选择 IE 浏览器的“工具”→“Internet 选项”命令，打开“Internet 选项”对话框，选择“常规”选项卡，单击“删除”按钮。然后在弹出的“删除浏览的历史记录”对话框中选中“历史记录”复选框，单击“删除”按钮。

第 4 步：清除访问过的网站地址。

在“Internet 选项”对话框中选择“内容”选项卡，单击“设置”按钮，如图 9.5 所示。然后在弹出的“自动完成设置”对话框中取消选中“地址栏”复选框，如图 9.6 所示。这样就无法通过使用部分地址匹配的方法打开曾经访问过的 Web 站点了。

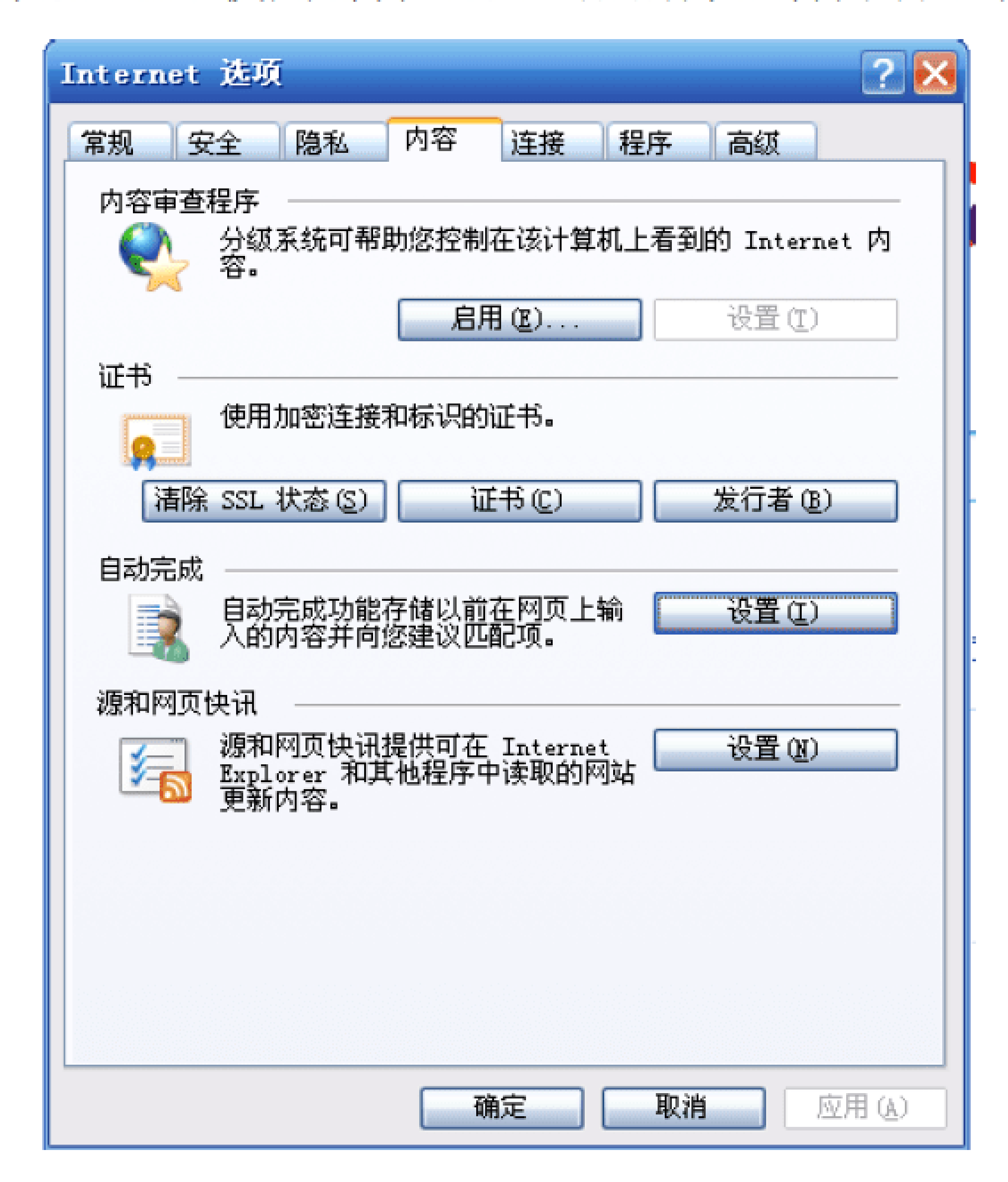


图 9.5　“内容”选项卡

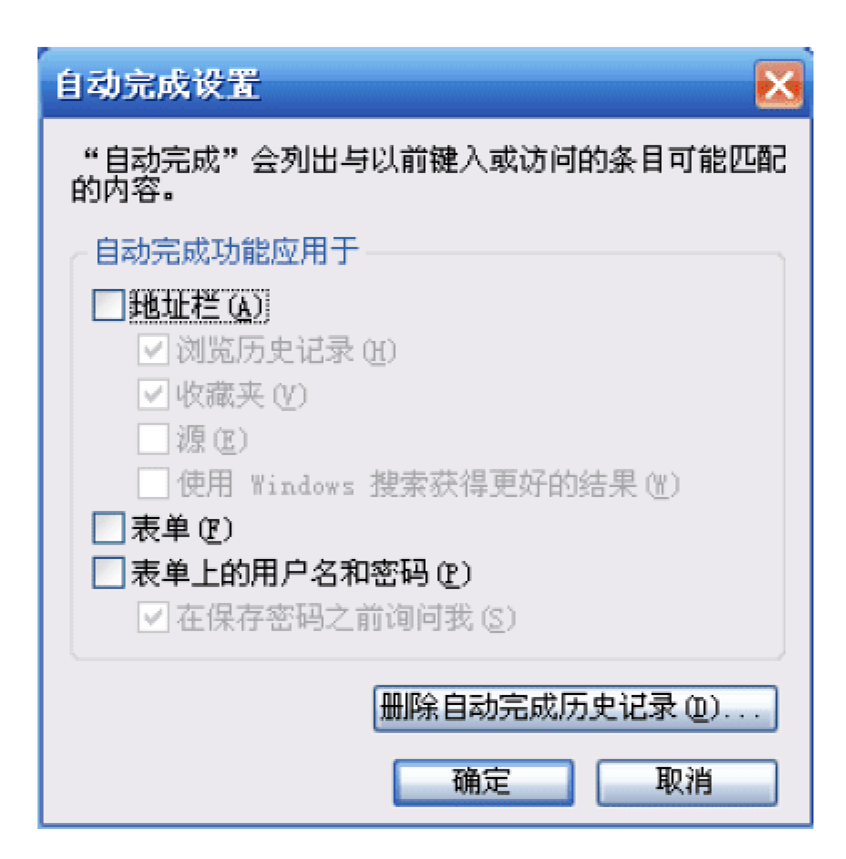


图 9.6　“自动完成设置“对话框

第 5 步：清除 IE 记住的表单和表单密码。

选择 IE 浏览器的“工具”→“Internet 选项”命令，打开“Internet 选项”对话框，选择“常规”选项卡，单击“删除”按钮。然后在弹出的“删除浏览的历史记录”对话框中选中“表单数据”复选框，单击“删除”按钮，如图 9.7 所示。

选择 IE 浏览器的“工具”→“Internet 选项”命令，打开“Internet 选项”对话框，选择“常规”选项卡，单击“删除”按钮。然后在弹出的“删除浏览的历史记录”对话框中选中“密码”复选框，单击“删除”按钮，如图 9.8 所示。

第 6 步：删除 Cookie 内容。

Cookie 是一种发送到客户端浏览器的文本串句柄，并保存在客户机硬盘上，很容易暴露用户信息，给用户带来不安全因素。通过以下操作可以禁用 Cookie。

选择 IE 浏览器的“工具”→“Internet 选项”命令，打开“Internet 选项”对话框，选择“常规”选项卡，单击“删除”按钮。然后在弹出的“删除浏览的历史记录”对话框中选中 Cookie 复选框，单击“删除”按钮确认，如图 9.9 所示。



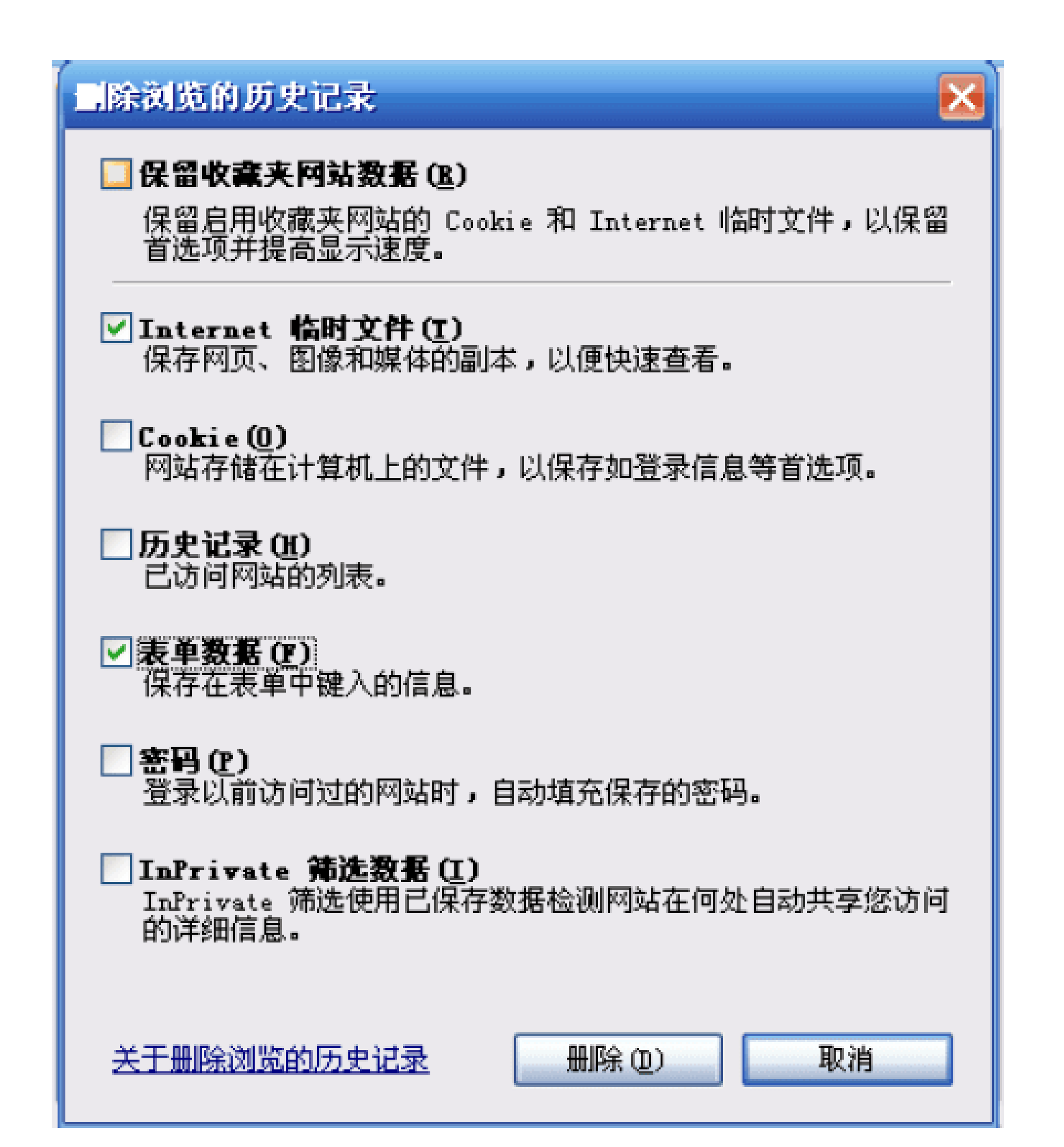


图 9.7　清除表单的设置

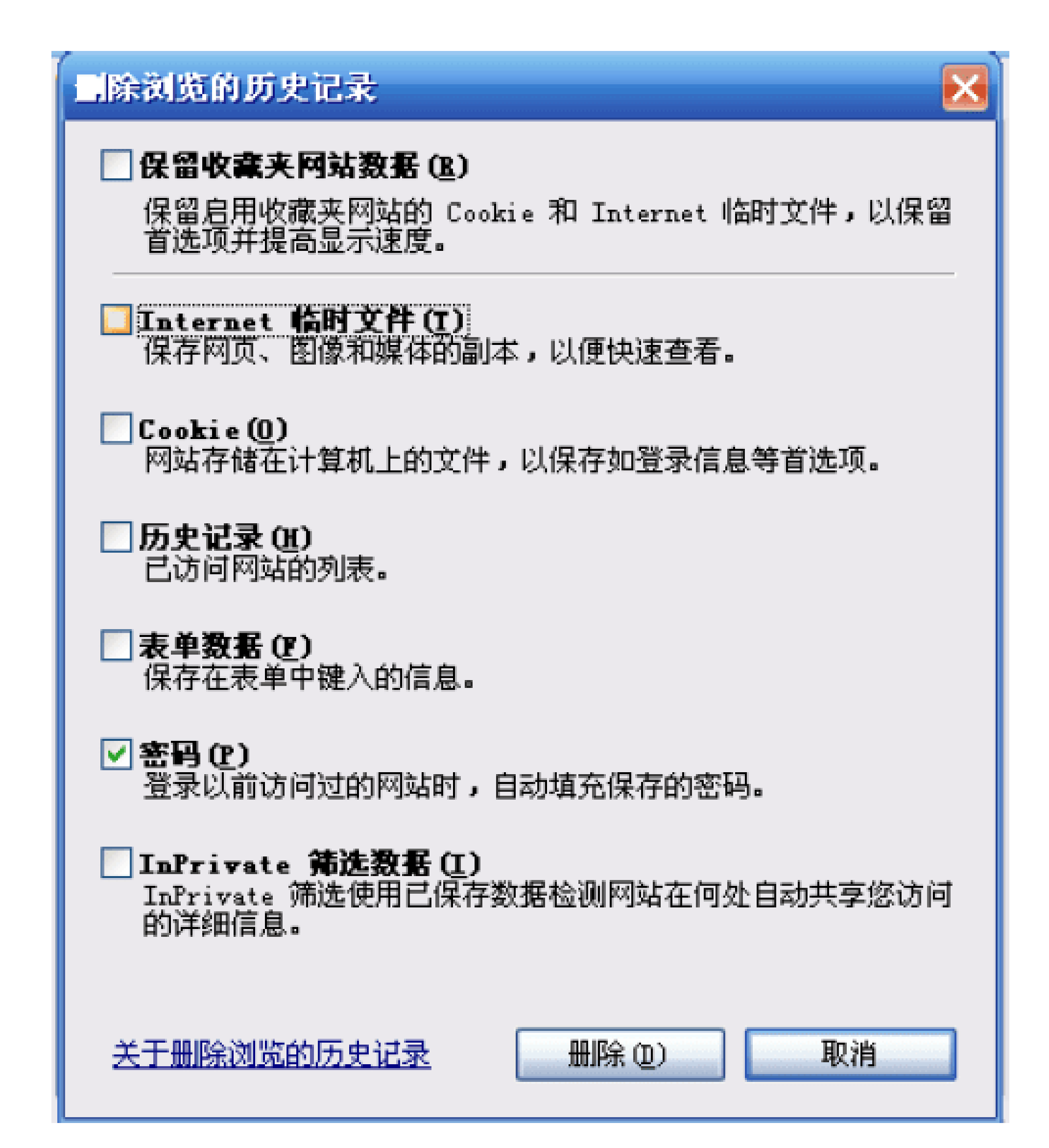


图 9.8　清除密码的设置

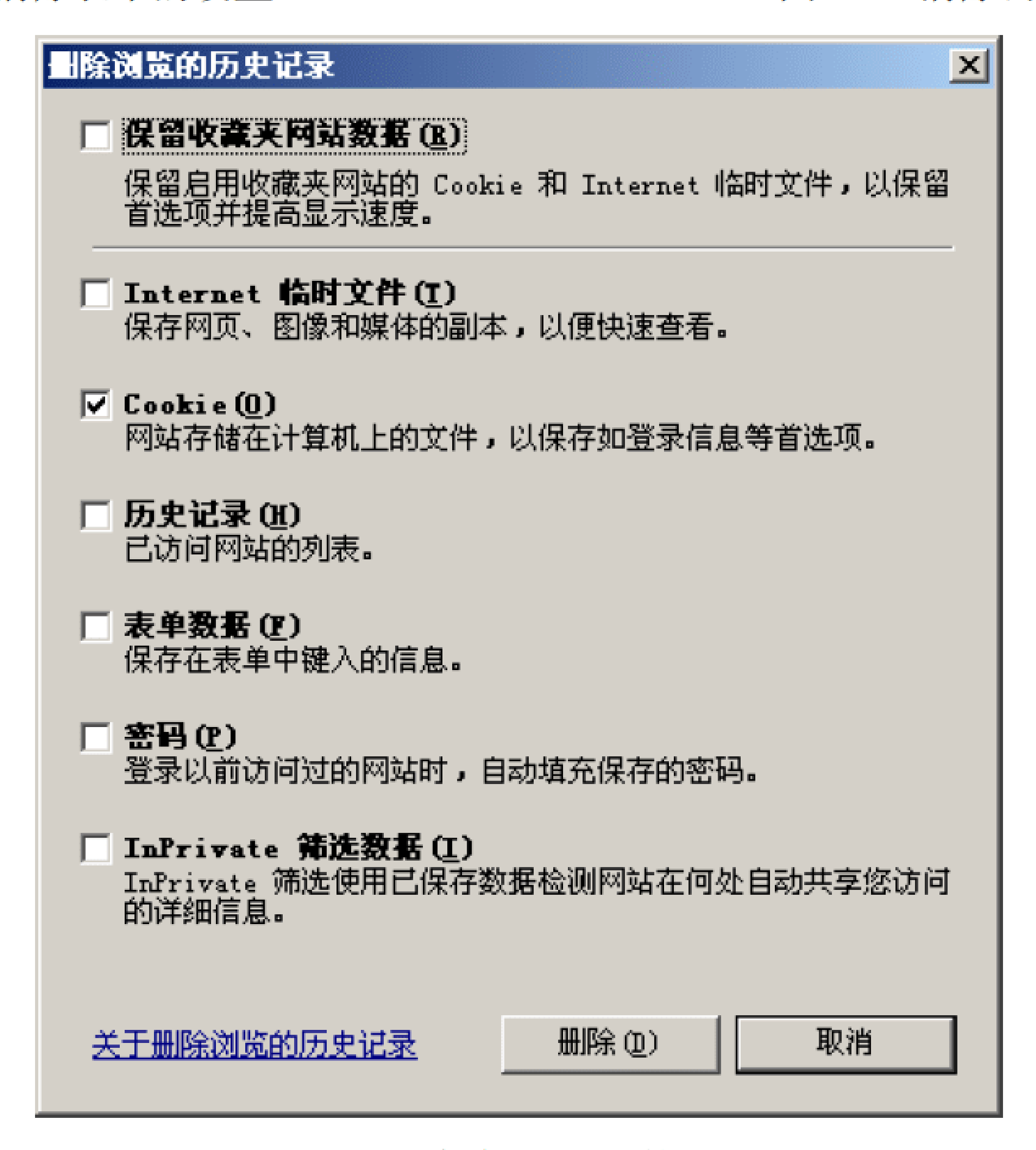


图 9.9　清除 Cookie 的设置

实训 2　Web 服务器安全配置

实训目的

掌握提高 Web 服务器安全性的设置方法。

实训环境

安装了 Windows Server 2003 操作系统的服务器。



操作步骤

第 1 步：启用过期内容。

启用过期内容就是指通过设置来保证自己的站点的过期信息不被发布出去。

（1）在“默认网站 属性”对话框中选择“HTTP 头”选项卡，如图 9.10 所示。在该选项卡中，选中“启用内容过期”复选框，激活“启用内容过期”选项区域中的选项。

（2）在“启用内容过期”选项区域中，用户可以设置内容的过期时间。

第 2 步：内容分级设置。

如果用户站点的内容并不是针对所有的访问者，需要进行内容分级设置，以防止不具备分级要求的其他访问者查看站点内容。在预设的情况下，Windows Server 2003 启用的是 RSAC（Recreational Software Advisory Council）分级服务系统进行分级服务。该 Internet 分级是斯坦福大学的 Donald F. Roberts 博士研究的，它主要针对暴力、性、裸体和语言 4 个方面进行分级设置。在设置分级服务内容前，用户需要上网填写一个 RSAC 分级问卷，以获得一些推荐的内容分级，以便更好地进行分级设置。分级内容的设置过程如下：

（1）在图 9.10 中单击“编辑分级”按钮，打开“内容分级”对话框，如图 9.11 所示。

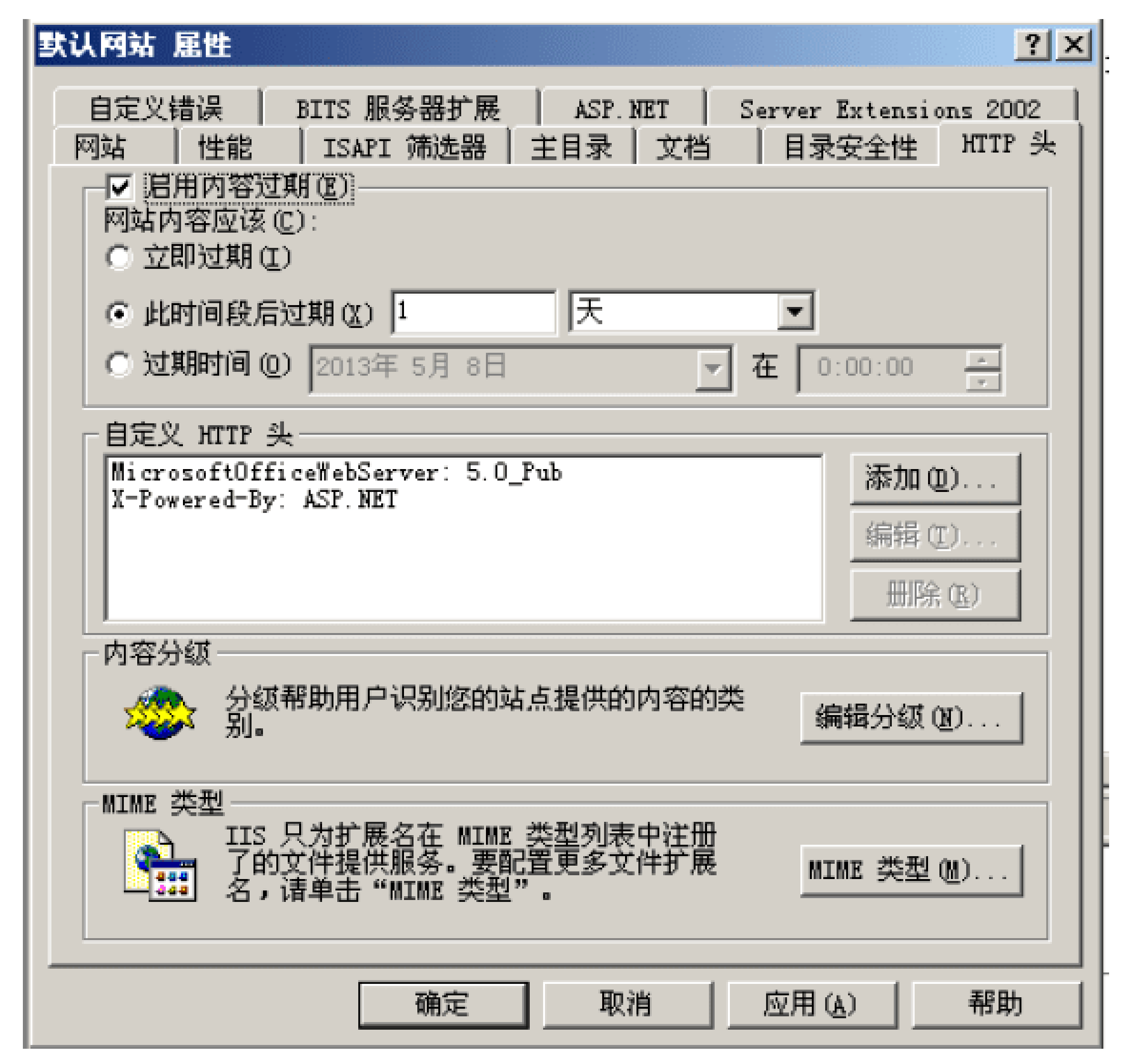


图 9.10　“HTTP 头”选项卡

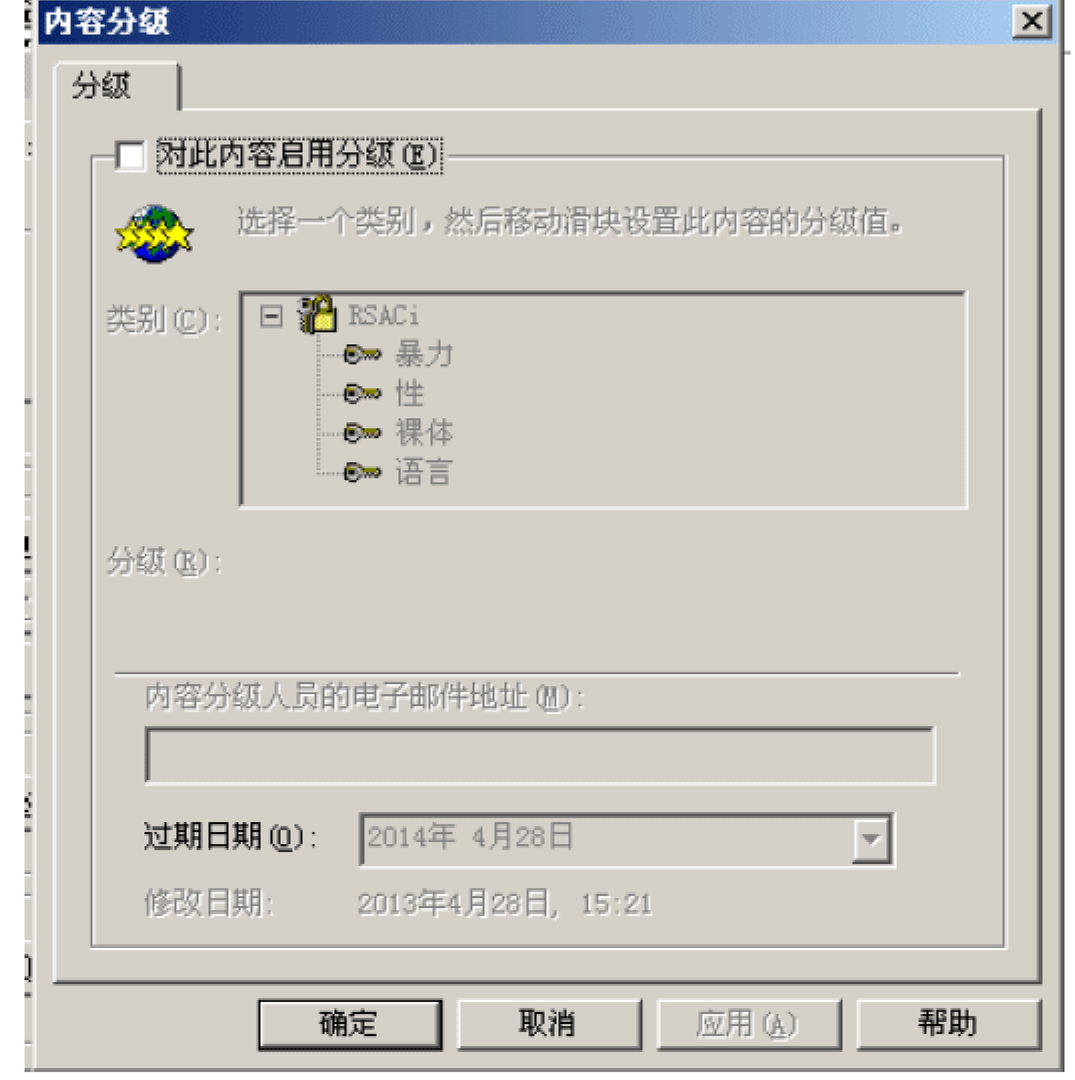


图 9.11　“内容分级”对话框

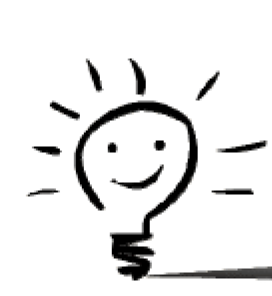
（2）用户可以在此设置分级服务的内容，以过滤公司的 Web 页的内容。选择“分级”选项卡，并选中“对此内容启用分级”复选框，如图 9.12 所示。

（3）在“类别”列表框中，选择暴力、性、裸体和语言 4 个类别中的一种，分级滑块就会显示出来，调节该滑块，可改变所选类别的分级级别。

（4）如果希望对自己的电子邮件进行分级服务，可以在“内容分级人员的电子邮件”文本框中输入自己的电子邮件地址。

（5）如果希望单独为分级服务设置失效时间，可单击“过期日期”下拉列表框中的下三角按钮，从弹出的日历中选择一个日期。

（6）设置好之后，单击“确定”按钮返回到“默认网站属性”对话框，再单击“确定”



按钮，保存设置。

第 3 步：添加网页页脚。

在 Web 站点管理中，用户经常在每一个 Web 页的前面插入一个由 HTML 语言编写的脚本文件，作为网页页脚，以增加 Web 站点的内容。

（1）创建一个 HTML 网页页脚文件，并把它保存在自己的 Web 服务器所在的硬盘上。

（2）在 Internet 服务管理器的控制台目录树中，右击某一个 Web 站点或者目录子节点，例如，右击默认网站，从弹出的快捷菜单中选择“属性”命令，打开“默认网站 属性”对话框，选择“文档”选项卡，如图 9.13 所示。

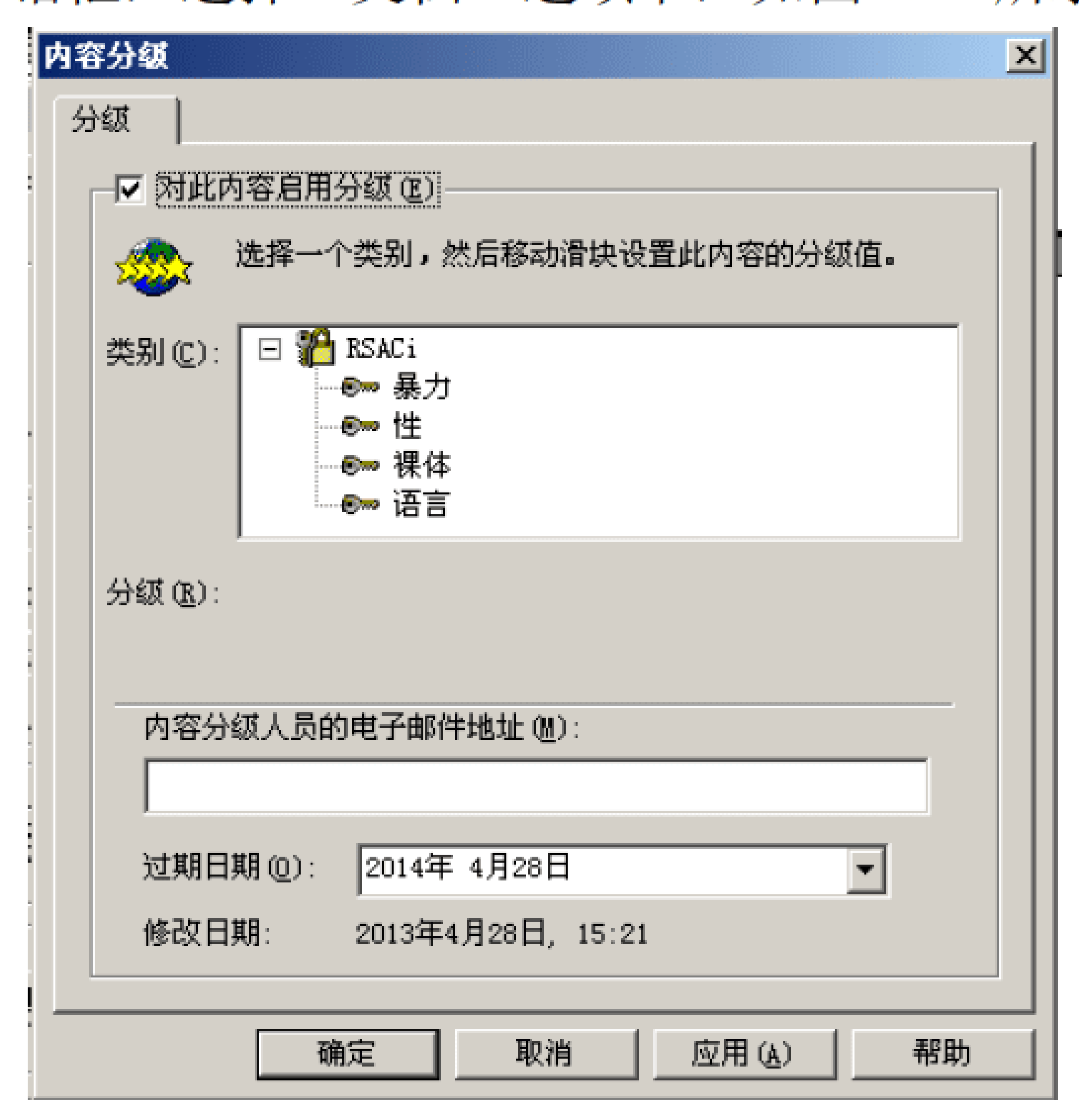


图 9.12 “分级”选项卡

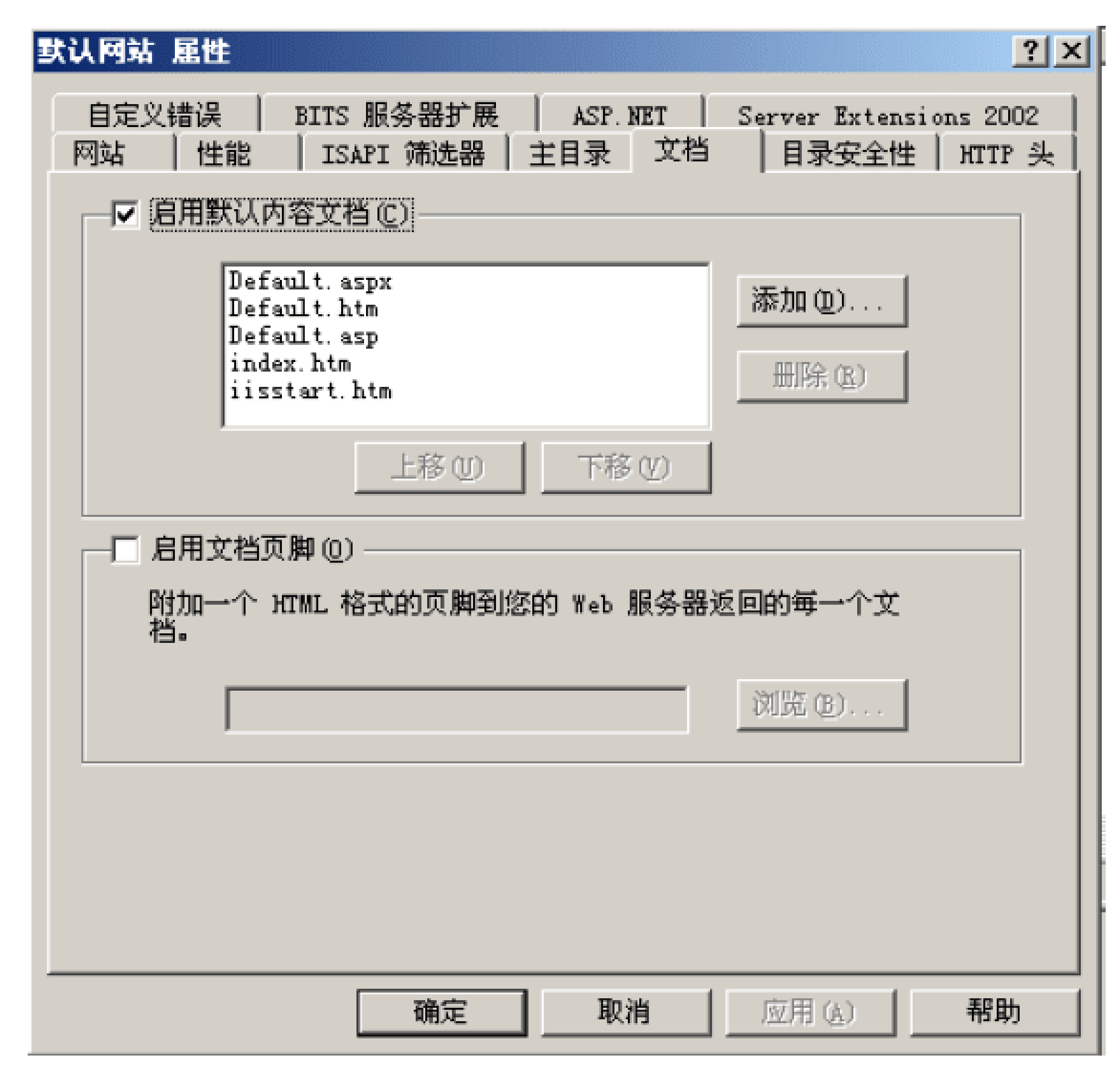


图 9.13 “文档”选项卡

（3）在“文档”选项卡中，选中“启用文档页脚”复选框，在对应文本框中输入页脚文件的完整路径。如果用户不知道页脚文件的完整路经，可单击“浏览”按钮，打开“打开”对话框进行选择。

（4）单击“确定”按钮，返回到属性对话框，再单击“确定”按钮保存设置。

第 4 步：安全认证。

在 Windows Server 2003 中，对于通过 HTTP 协议访问，Internet 信息服务提供了 3 种登录认证方式，它们分别是匿名方式、明文方式和询问/应答方式。采用哪种方式取决于用户建立 Internet 信息服务器的目的。

由于在许多 Internet 信息服务器上，对 Web、FTP 及 SMTP 虚拟服务器的访问都是匿名的，下面以匿名访问为例介绍如何进行安全认证设置。

（1）在如图 9.14 所示的对话框中选择“目录安全性”选项卡。

（2）在“身份验证和访问控制”选项区域中单击“编辑”按钮，打开“身份验证方法”对话框，如图 9.15 所示。

（3）要选择匿名认证方式，选中“启用匿名访问”复选框，并单击“浏览”按钮，打开如图 9.16 所示的“选择用户”对话框进行设置。



图 9.14　“目录安全性”选项卡

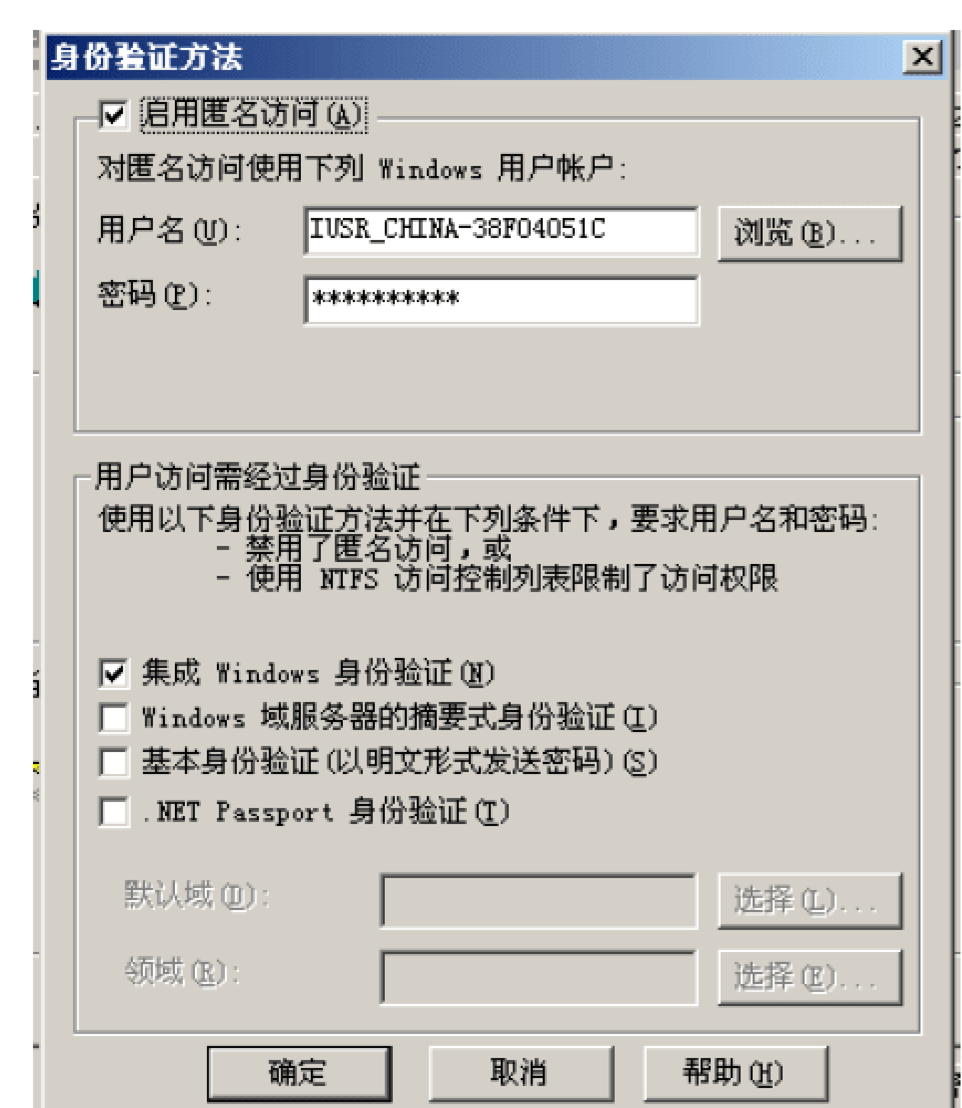


图 9.15　设置身份验证和访问控制

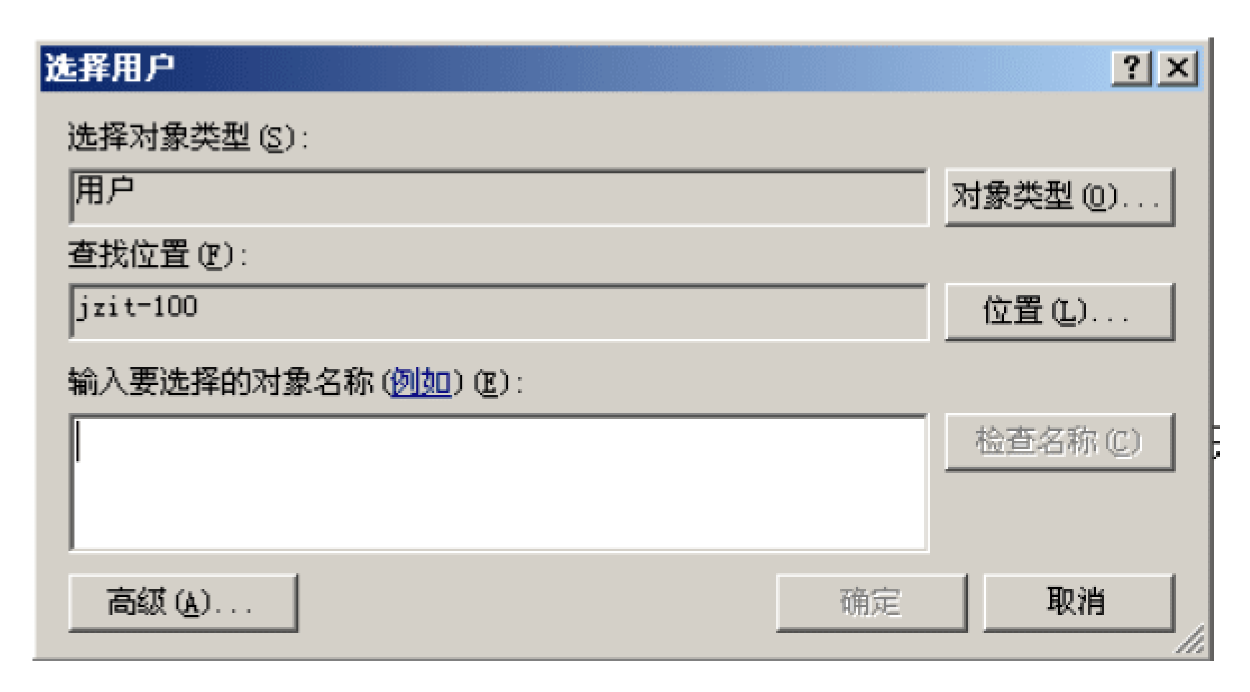


图 9.16　“选择用户”对话框

（4）在安装 Internet 信息服务时，系统将自动创建一个匿名账号：IUSR 计算机名，如果计算机名为 LY，则匿名账号为 IUSR_LY。使用“IUSR 计算机名”账号可以将 Web 客户登录到服务器上。允许匿名服务时，管理员可更改用户匿名请求的用户账号，并可更改此账号的密码。在“用户名”文本框中直接输入用户账号，或者单击“浏览”按钮，打开如图 9.17 所示的“选择用户”对话框，选择一个要添加的用户账号。

（5）在“身份验证方法”对话框中，选中“启用匿名访问”复选框，或者在“密码”文本框中输入用户账号密码。

（6）单击“确定”按钮完成匿名访问设置，返回到“默认网站 属性”对话框，然后单击“确定”按钮关闭对话框。

第 5 步：IP 地址及域名限制。

通过 IP 地址及域名限制，用户可禁止某些特定的计算机或者某些区域中的主机对自己的 Web 和 FTP 站点及 SMTP 虚拟服务器的访问。当有大量的攻击和破坏来自于某些地址或者某个子网时，使用这种限制机制是非常有用的。不过，进行 IP 地址及域名限制的首要条件是用户必须知道网络黑客的计算机使用哪些 IP 地址或属于哪些网络区域，否则无法进

行限制。对基于 Internet 的信息服务器，站点接受来自于各方的访问，用户很难进行地址限制。一般来说，只有基于企业内部网络的信息服务器才使用 IP 地址及域名进行安全保护。下面以 Web 站点为例进行 IP 地址及域名限制的设置。

（1）在图 9.14 的“IP 地址和域名限制”选项区域中，单击“编辑”按钮，打开“IP 地址和域名限制”对话框，如图 9.18 所示。



图 9.17　选择用户

（2）如果选中“授权访问”单选按钮，除了“下列除外”列表框中的计算机外，其他所有的计算机都可访问该 Web 站点上的内容；如果选中“拒绝访问”单选按钮，除了“下列除外”列表框中的计算机外，其他所有的计算机都不能访问该 Web 站点上的内容。这里选中“授权访问”单选按钮并添加没有访问权限的计算机。

（3）单击“添加”按钮，打开“拒绝访问”对话框，如图 9.19 所示。







图 9.18　设置 IP 地址和域名限制　　　　图 9.19　“拒绝访问”对话框

（4）如果要对单个计算机进行限制，选中“一台计算机”单选按钮，并在“IP 地址”文本框中输入要授权的计算机的 IP 地址；或者单击“DNS 查找”按钮，打开“DNS 查找”



对话框，选择某个 DNS 域中要授权的计算机。如果要对一组计算机进行限制，选中“一组计算机”单选按钮，在“网络标识”文本框中输入要授权的一组计算机中的任何一个计算机的 IP 地址，并在“子网掩码”文本框中输入子网掩码。如果要对某个域中的计算机进行限制，选中“域名”单选按钮，并在“域名”文本框中输入授权的域名。

（5）单击“确定”按钮返回到“IP 地址和域名限制”对话框。如果还要进行访问授权，可继续单击“添加”按钮进行添加。这样，被添加的单个计算机、一组计算机或者一个域的客户可访问服务器，而其他的客户则没有访问权。

（6）单击“确定”按钮返回到“默认站点 属性”对话框，再单击“确定”按钮保存设置。

第 7 步：停止、启动和暂停站点服务。

在站点维护中，停止、启动和暂停站点服务是经常要进行的工作。例如，当某个站点的内容和设置需要进行比较大的修改时，用户可将该站点的服务停止或者暂停，以便操作。当已经停止或暂停的站点需要启动自己的服务时，就启动它。

要停止、启动和暂停某个站点的信息服务，在控制台目录树中，展开“ Internet 信息服务”节点和服务器节点。如果要暂停某个 Web 或者 FTP 站点服务，右击该站点，在弹出的快捷菜单中选择“暂停”命令即可；如果要停止某个 Web 或者 FTP 站点服务，右击该站点，在弹出的快捷菜单中选择“停止”命令即可；如果要启动某个已经暂停或者停止的 Web 或者 FTP 站点服务，右击该站点，在弹出的快捷菜单中选择“启动”命令即可。

参 考 文 献

1．蔡立军．计算机网络安全技术．北京：中国水利水电出版社，2002
2．方勇，刘嘉勇．信息安全导论．北京：电子工业出版社，2003
3．顾巧论．计算机网络安全．北京：科学出版社，2003
4．蒋建春，冯登国．网络入侵检测系统的设计与实现．北京：电子工业出版社，2002
5．焦树海．计算机安全概论．天津：南开大学出版社，2004
6．李海泉，李健．计算机系统安全技术．北京：人民邮电出版社，2001
7．宋红．计算机安全技术．北京：中国铁道出版社，2007
8．徐卓峰．信息安全技术．武汉：武汉理工大学出版社社，2004
9．张小斌．计算机网络安全工具．北京：清华大学出版社，1999
10．张永平．计算机系统安全技术．北京：高等教育出版社，2003
11．钟乐海．网络安全技术．北京：电子工业出版社，2006
12．刘远生，辛一．计算机网络安全．北京：清华大学出版社，2009
13．韩最蛟．网络维护与安全技术教程与实训．北京：北京大学出版社，2008
14．吴辰文．网络安全教程及实践．北京：清华大学出版社，1012
15．冯登国，徐静．网络安全原理与技术．北京：科学出版社，2010
16．刘天华，孙阳，朱宏峰．网络安全．北京：科学出版社，2010
17．薛庆水，朱元忠．计算机网络安全技术．大连：大连理工大学出版社，2008